AFRICAN WOMEN'S DEVELOPMENT FUND

CRAWN TRUST
Community Advocacy and Awareness Trust

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

TABLE OF CONTENTS

Statement of Principle....1
Executive Summary....1
CHAPTER 1 — Background and Rationale for a Strategic Intervention....4
1.1 The Digital Frontier: A Paradox of Progress and Peril....4
1.1.1 From the Cradle of Humankind to the Cradle of Innovation....4
1.1.2 The Pillars of Kenyan Innovation....4
1.1.3 The Double-Edged Sword of the Silicon Savannah....4
1.1.4 The Democratic and Economic Cost of Digital Silencing....4
1.2 Understanding Technology-Facilitated Gender-Based Violence....5
1.3 The Continuum Between Online Harm and Offline Violence....6
1.4 Democratic Participation, Leadership and the Silencing of Women....6
1.5 Economic and Development Implications of TFGBV....8
1.6 Why a Legislative and Institutional Gap Analysis is Required....9

CHAPTER 2 — Review of Existing Legal and Policy Frameworks: Gaps and Required Amendments 19
Domestic Legal Instruments....20
2.1 The Constitution of Kenya (2010)....10
2.2 The Computer Misuse and Cybercrimes Act (CMCA)....10
2.3 The Data Protection Act (DPA)....15
2.4 The Sexual Offences Act....18
2.5 The Penal Code (Cap. 63)....18
2.6 The Evidence Act (Cap. 80) and Digital Evidence Standards 18
2.7 Kenya Information and Communications Act (KICA)....19
2.8 The Protection Against Domestic Violence Act (PADVA)....21
2.9 The Victim Protection Act (VPA)....22
2.10 The Children Act....23
2.11 The Employment Act (Sexual Harassment Provisions)....24
2.12 The Media Council Act....24
2.13 The National Cohesion and Integration Act (NCIA)....25
2.14 The National Gender and Equality Commission Act....26
2.15 The Artificial Intelligence Bill (2026)....26

Regional and International Frameworks: Alignment and Implementation Gaps.... 27
2.16 The African Charter on Human and Peoples' Rights....27
2.17 The Maputo Protocol....28
2.18 The AU Convention on Ending Violence Against Women and Girls (2025)....28
2.19 CEDAW and General Recommendation No. 35....29

CHAPTER 3 — Stakeholder Consultation Findings....32
3.1 Overview of Consultation Methodology....32
3.2 Institutional Challenges Identified by Stakeholders....33
3.3 Platform Accountability and Content Moderation Challenges....34
3.4 Access to Justice Barriers....35
3.5 Emerging Technology Concerns Raised by Stakeholders....35

CHAPTER 4 — Key Informant Questionnaire Analysis.....36
4.1 State Actors and Constitutional Office Holders.....38
4.2 Civil Society Organizations and Feminist Groups.....38
4.3 Survivor Experiences: Questionnaire Findings from the Wangu Kanja Foundation.....39

CHAPTER 5 — Integrated Thematic Gap Analysis..44
5.1 Definitional and Legislative Gaps.....44
5.2 Enforcement and Evidentiary Gaps.....45
5.3 Institutional Coordination Gaps.....45
5.4 Survivor Remedy and Redress Gaps.....45
5.5 Awareness and Prevention Gaps.....45
5.6 Child Protection Gaps.....45
5.7 Intersectional Vulnerability Gaps.....46
5.8 Demographic Disaggregation: Intersecting Vulnerabilities.....46

CHAPTER 6 — Emerging Technology and Future Risk Landscape.....50
6.1 Artificial Intelligence and Synthetic Media.....50
6.2 Voice Cloning and Deepfake Risks.....50
6.3 Cryptocurrency and Sextortion.....50
6.4 Quantum Computing and Future Evidence Challenges.....50
6.5 Elections, Democracy and AI-Enabled Disinformation.....51

CHAPTER 7 — Recommendations and Reform Roadmap.....53
7.1 Legislative Reform Priorities.....54
7.2 Institutional Strengthening.....54
7.3 Survivor-Centred Justice and Remedies.....55
7.4 Platform Accountability and Regulatory Reform.....55
7.5 Public Awareness and Prevention.....55
7.6 Child Online Protection.....55
7.7 AI Governance and Emerging Technology Regulation.....55
7.8 Artificial Intelligence Bill – Required Amendments.....56
7.9 Socio-Economic Wellbeing: Cross-Cutting Recommendations.....56
CONCLUSION.....57
List of Acronyms and Abbreviations.....58
Section 1 — Domestic Legislation and Legal Instruments.....58
Section 2 — Kenyan Institutions, Bodies and Offices.....60
Section 3 — International and Regional Frameworks.....61
Section 4 — International Organizations and Research Bodies.....63
Section 5 — Subject Matter Terms and Technical Concepts.....65

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, 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 to support rights-based, women-led initiatives that challenge structural inequality and systemic violence. It is grounded in the Constitution of Kenya (2010) 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.

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 centred 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 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 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 and cryptocurrency enabled sextortion. 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), 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 data collection practices, while child specific provisions are absent from the Artificial Intelligence Bill 2026. TFGBV against girls therefore 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 from the Constitution to the National Gender and Equality Commission Act and fourteen regional and international frameworks from the Maputo Protocol to 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, significant amendment is required 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, vote, professional contribution and democratic perspective that Kenya's knowledge economy cannot afford to lose.

MUTHEU NYAGAH KHIMULULLM. Cyber Security, Counter Terrorism & Crisis Management
https://www.linkedin.com/in/mutheu-khimulu-law/
Lead Consultant, Gap Analysis on TFGBV in Kenya
April 2026.

CHAPTER ONE

BACKGROUND AND RATIONALE FOR A STRATEGIC INTERVENTION.

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

Kenya is uniquely defined by a dual heritage: it is recognized globally as the Cradle of Humankind, holding the most diverse record of human evolutionary history (from the 7-million-year-old Orrorin tugenensis to the Turkana Boy), and has now ascended as the Cradle of Innovation due to its modern landscape in pioneering homegrown, "leapfrog" technologies that reshape global industries.

1.1.2 The Pillars of Kenyan Innovation:

Kenya's ascent as a tech powerhouse is anchored by two revolutionary exports i.e., Ushahidi and M-Pesa. Ushahidi is a Kenyan-made crowdsourcing engine that redefined digital activism and disaster response. Its impact is global and it was famously deployed by the 2012 Obama Presidential Campaign to map voter suppression in real-time and utilized by the U.S. Marine Corps and Coast Guard to direct life-saving aid during the Haiti earthquake.

Perhaps the most striking evidence of Kenya's ingenuity, is M-Pesa as this financial revolution achieved a world-leading 91% market penetration. By successfully "banking the unbanked," M-Pesa was ranked by the Project Management Institute as the 9th 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 a staggering 149.4%, thereby reflecting a society where SIM registrations have climbed past 78 million and mobile money penetration holds steady at 91% (CA First Quarter Sector Statistics 2025/2026). However, this digital transformation represents a profound paradox.

While these metrics signal unprecedented platforms for economic agency and voice, they simultaneously delineate a vast, expanded "attack surface" for Technology-Facilitated Gender-Based Violence (TFGBV). In this Cradle of Innovation, the very tools that have propelled Kenya to become the world's 9th fastest-growing digital economy are now being weaponized with terrifying precision. Consequently, the same digital transformation that offers revolutionary empowerment, is also being exploited to target and silence, turning the country's most celebrated democratic and financial advancements, 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 effect" or "radio silencing" of girls and women has far-reaching implications including:

- 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.

Tragically, this harm often escalates into physical violence, bodily harm, and even death. This is frequently facilitated through the misuse of digital tools within intimate relationships to monitor, control, or systematically dismantle a victim's reputation and livelihood.

These violations are further compounded by the weaponization of emerging technologies, such as AI-generated deepfakes and the non-consensual dissemination of intimate content (NCII).

A harrowing example of this is the recent, widely publicized case involving a Russian national who allegedly recorded and leaked intimate content of numerous Kenyan women without their consent. The fallout from this case, , underscores how digitally-mediated violations can lead to irreversible trauma, profound reputational ruin, and devastating personal loss. In response to the public outcry and the severity of these allegations, Kenyan law enforcement and cybercrime authorities have launched a formal investigation into the Russian national's activities to address the cross-border nature of these digital violations and seek justice for the affected women.

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.

Accordingly, TFGBV must be framed not only as a safety and human rights issue, but also 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):

A comprehensive conceptual understanding of Technology-Facilitated Gender-Based Violence (TFGBV) is imperative to address its status as a critical, yet inadequately regulated, threat to the socio-economic advancement of women and girls. To this end 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.

It 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.

According to UN Women, online and technology-facilitated violence against women constitutes a form of gender-based violence that includes "acts of violence committed, assisted or aggravated by the use of information and communication technologies" and should be understood as part of the broader continuum of violence against women and girls rather than as a separate or lesser harm.

The Association for Progressive Communications (APC) conceptualizes TFGBV as a pattern of psychological, emotional, sexual, economic, and reputational harm carried out through digital means. APC emphasizes that TFGBV is defined not merely by the technology used, but by the gendered intent, impact, and power relations underlying the abuse. Forms of TFGBV identified by APC include non-consensual sharing of intimate images, cyberstalking, online harassment, impersonation, doxing, sextortion, and coordinated misogynistic attacks.

The UN Special Rapporteur on Violence Against Women and UNESCO have further recognized that digital technologies introduce distinct characteristics to gender-based violence, including scale, permanence, anonymity, transnational reach, and algorithmic amplification. These features can exacerbate harm, impede access to justice, and silence women's participation in public, political, and civic life, particularly for women journalists, politicians, and human rights defenders.

At the regional level, the African Commission on Human and Peoples' Rights (ACHPR), through Resolution 522 on the Protection of Women Against Digital Violence in Africa, explicitly recognizes digital and online violence as a human rights violation. The Resolution defines digital violence broadly to include acts committed through digital tools that result in physical, sexual, psychological, or economic harm to women and girls 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:

Additionally, contemporary understandings of TFGBV now extend to emerging and AI-enabled harms, including AI-generated deepfake sexual images, nudify and synthetic image applications, voice cloning, gendered disinformation, and automated harassment. These forms of abuse expose significant gaps in existing legal, regulatory, and institutional frameworks, particularly in relation to:

- **Attribution:** The difficulty of identifying perpetrators behind automated or synthetic content, as well as the proliferation of pseudo-accounts used to execute coordinated attacks with impunity.
- **Evidence Preservation**: The challenge of freezing volatile digital evidence before it is deleted or altered by algorithms.
- **Jurisdiction:** The borderless nature of AI platforms that often operate outside Kenyan territory
- **Survivor Remedies:** The lack of specific right to be forgotten or rapid takedown mechanisms for AI-generated harms.

1.2.3 From Legal Frameworks to Lived Reality:

While legal and policy frameworks provide a formal structure for addressing TFGBV, a critical gap persists between law as written and law as experienced.

The lived experiences of survivors and the professional insights of practitioners engaged during this analysis provide a clear consensus that there are:

- Low reporting rates due lack of awareness on where and how to report, fear of retaliation, stigma, and lack of trust in enforcement mechanisms.
- Procedural barriers and delays in obtaining digital evidence preservation and platform cooperation.
- Limited awareness among survivors of available legal remedies and reporting channels.

Bridging this gap requires integrating lived experiences, survivor testimony, and practitioner expertise into legal and policy reform.

1.3 THE GENDERED GEOGRAPHY OF RISK:

MAPPING THE "RADIO SILENCING" OF KENYAN WOMEN.

1.3.1 The Weaponization of Digital Innovation:

The digital transformation of the "Silicon Savannah" has birthed a paradoxical landscape where the tools of innovation have been repurposed into weapons of exclusion. Current evidence suggests that digital spaces are being systematically weaponized to purge women from the public sphere, creating a chilling effect that transcends the digital-physical divide. This "radio silencing" is not a peripheral issue; it is a systemic threat to democratic participation and bodily autonomy, manifesting across three critical demographics:

- **The Academic Frontline (Tertiary Institutions)**: A landmark UNFPA 2024 study reveals that nearly 90% of young adults in Nairobi's higher learning institutions have witnessed TFGBV. The victimization is starkly gendered i.e., 64.4% of female students have personally experienced online violence, which is nearly double the rate of their male peers at 35.5% (UNFPA/CCGD 2024).
- **The Political and Media Vanguard (Women in Public Life)**: For women leaders, journalists, and activists, digital hostility is a tool of political censorship. According to an Inter-Parliamentary Union (IPU) survey, 80% of women parliamentarians in Africa have faced psychological violence online. Furthermore, a UNESCO 2025 global report indicates that 75% of women media workers report digital abuse while performing their duties, directly contributing to a 63% increase in self-censorship (UNESCO 2025).
- **The Rural-Urban and Socio-Economic Divide:** While mobile ownership approaches parity, rural women (48.6% ownership) face unique vulnerabilities such as economic tech-abuse. In these contexts, partners often control phone access or M-Pesa credentials, as a form of tech-enabled violence, which is reported by 31.1% of women in regional audits (Johns Hopkins Bloomberg School 2024).

1.3.2 The Lethal Continuum: From Digital Threats to Femicide:

It is imperative to note the psychological and physical links inherent in this data. 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 (UNESCO/Police Report 2025). From the non-consensual sharing of intimate imagery (NCII) to the rapid rise of AI-driven deepfakes, which now account for 98% of all online deepfake content (EPRS 2025), digital harm is currently outpacing the state's legislative capacity.
In this Cradle of Innovation, the same technologies Kenya helped pioneer are being weaponized to erode the digital sovereignty of its citizens, demanding a "Future-Back" legal framework that can keep pace with the evolving nature of these attack vectors.

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 impacts:

- Academic participation and online learning engagement.
- Professional networking and digital career development.
- Retention of women in STEM, digital entrepreneurship, and public leadership pathways.

This in turn creates a long-term pipeline risk for Kenya's digital economy and innovation leadership, as the radio silencing of women results in a homogenized knowledge base, that lacks the diverse insights necessary to build inclusive tech solutions, ultimately leaving Kenyan products less competitive in a global market that demands gender-responsive innovation.

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 recognizes a broad spectrum of TFGBV, ranging from established cybercrimes to emerging AI-driven threats including:

- **Cyberstalking & Surveillance:** This perpetuated via the use of GPS tracking, stalkerware, or persistent digital monitoring. Under Section 27 of the Kenya Computer Misuse and Cyber Crimes Act (CMCA), "cyber-harassment" is criminalized, nevertheless specific provisions for sophisticated surveillance remain a grey area.
- **Doxing:** This is the malicious publication of private identifying information for example, home addresses or phone numbers, to incite real-world harassment, often bypassing the Kenya Data Protection Act's "legitimate interest" clauses.
- **Non-Consensual Sharing of Intimate Imagery (NCII)**: This involves the distribution of private sexual images to humiliate or extort. Section 37 of the CMCA specifically penalizes this, yet enforcement remains hampered by the 2025 High Court suspensions on related harassment clauses in the case of Reuben Kigame Lichete & Kenya Human Rights Commission (KHRC) vs. The Attorney General & Others (HCCRPET/E673/2025).
- **Gendered Disinformation:** Entails coordinated campaigns using false narratives to silence women in public life. This is a direct threat to the Maputo Protocol's guarantee of women's right to participate in political processes.
- **AI-Enabled Abuse**: Encompasses the use of Generative AI for voice cloning and the creation of deepfake sexual imagery, which is also known as deepfake weaponization. Currently, 98% of all deepfake content online is non-consensual sexual imagery targeting women as was noted in the European Parliamentary Research 2025. Moreover, there is an algorithmic bias in the making because, without intervention, Kenya's National AI Strategy 2025–2030 risks being gender-blind, thereby allowing automated systems to further marginalize women. That is why this gap analysis adopts a "Future-Back" approach to ensure policy keeps pace with emerging technologies like AI-enabled voice cloning and nudify apps.

1.4.2 The Withdrawal from Digital Civic Space:

Evidence indicates that sustained exposure to online abuse leads many women to self-censor, disengage, or abandon digital platforms entirely. This withdrawal results in:

Reduced representation of women's voices in public debate.

Shrinking civic space and weakening of inclusive governance.

Increased normalization of online misogyny due to reduced counter-speech.

The cumulative effect is the systematic shrinking of digital civic space for women.

Additionally, there isthe "Ordinary User" Penalty that also arises when private citizens experience account takeovers, "hacking," or the non-consensual use of their likeness, it creates a climate of fear. This discourages everyday digital participation, reinforcing the idea that digital spaces are inherently unsafe for women.

1.4.3 The Legislative Gap: A Gender-Blind Architecture:

Despite the enactment of the Computer Misuse and Cybercrimes (Amendment) Act of 2024, Kenya's legal framework operates on a gender-neutral basis that often struggles to address the unique dynamics of Technology-Facilitated Gender-Based Violence (TFGBV).

Whilst the law correctly provides broad protections applicable to all genders, it lacks specific, gender-responsive provisions required to effectively prosecute the nuanced forms of digital harm that disproportionately affect women and girls.

This creates an enforcement crisis because, although "cyber-harassment" is criminalized under Section 27, these provisions are frequently challenged in court on constitutional grounds regarding their breadth and clarity. Consequently, the lack of specialized legal language and clear evidentiary standards results in an enforcement vacuum, leaving victims without adequate recourse despite the existence of the Act.

Furthermore, there is a "digital literacy" deficit, which is a critical mismatch between the sophistication of digital crimes and the technical capacity of duty-bearers. Many police officers and judicial officials lack the forensic training to handle electronic evidence or recognize the trauma inherent in digital violations.

1.4.4 Institutional and Capacity Constraints:

In addition to legislative gaps, institutional limitations continue to undermine enforcement, including:

- Limited specialized training for law enforcement, prosecutors, and judicial officers on digital evidence and TFGBV trauma.
- Insufficient forensic and technical infrastructure for handling electronic evidence.
- Fragmented coordination between regulators, law enforcement, and digital platforms.

This results in a persistent enforcement gap even where legal provisions exist.

1.4.5 The "Permanent Record" and Digital Trauma:

Unlike physical violence, digital violence is characterized by permanence. Once harmful content is uploaded, it becomes a "digital tattoo," thereby creating a state of perpetual victimization. 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.

By reclaiming these definitions through a feminist lens, this project seeks to shift the Kenyan narrative from "online trolling" to a serious breach of bodily autonomy and digital sovereignty

Ultimately, Technology-Facilitated Gender-Based Violence (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.

Driven by deep-seated structural inequality rather than technology alone, this evolving threat requires holistic, "Future-Back" responses that integrate:

- Feminist Legal Reform: Moving beyond gender-neutral laws to address the specific nuances of digital misogyny.
- Institutional Accountability: Strengthening the technical and gender-responsiveness of the Judiciary and the National Police Service (Policare).
- Platform Governance: Holding Big Tech and Internet Service Providers (ISPs) accountable for content moderation and rapid response.
- Survivor-Centred Justice: Prioritizing the agency, privacy, and long-term recovery of those targeted, while explicitly integrating mechanisms for restitution and compensation for both documented economic loss, and the profound injury to professional and personal reputation.

Whilst TFGBV targets individuals of all genders, including men and boys who may face 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 according to a report done by UN Women 2025.

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 our patriarchal African society, men and boys are often less protected by existing frameworks and may hesitate to report digital violations for fear of ridicule or perceived weakness; therefore, strengthening the overall digital justice system creates a safer environment for all survivors to seek recourse without the barriers of social stigma.

Crucially, our analysis recognizes that these harms are often systematically orchestrated within the manosphere, a digital ecosystem of misogynistic communities that weaponize algorithms to amplify 'red pill' ideologies and coordinated character assassinations. By centering this demographic, we address the most acute failure of our current digital safety frameworks, and confront the manosphere's role in normalizing the 'radio silencing' of women in public and professional life, ultimately working toward a truly inclusive and accountable Silicon Savannah.

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. 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. A complete analysis demands that policymakers and legislators understand the economic cost of inaction.

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

When women are systematically driven from digital spaces through TFGBV, the economic cost is not confined to individual survivors. Kenya's development strategy explicitly depends on the growth of a digital economy, knowledge services, and technology innovation. The UN Women Africa report of November 2025 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 because, it leads to a reduction in 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. When journalists self-censor beats relating to corruption, governance, and accountability to reduce the likelihood of coordinated digital attacks, the consequent reduction in investigative journalism capacity is an economic harm because, 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. Economic TFGBV encompasses the coercive control of women's access to M-Pesa credentials, the monitoring and interception of digital financial transactions as instruments of intimate partner control, the use of digital loan platforms to burden women with unauthorized debts, and the use of mobile financial platforms to execute financial fraud and extortion targeting women. A collaborative regional audit conducted by the Johns Hopkins Center for Global Women's Health and Gender Equity in partnership with the University of Nairobi WEE Hub and UNFPA Kenyapublished in 2024 documented that 31.1% of women in regional audits reported technology-enabled economic abuse by partners, including control over phone access and M-Pesa credentials.

As Kenya operationalizes the Virtual Asset Service Providers (VASP) Act 2025 and integrates emerging digital financial services (DFS) into its broader economic framework, the risk surface for technology-facilitated economic abuse will expand significantly. Current regulatory frameworks, including the Draft VASP Regulations 2026 and the Non-Deposit Taking Credit Providers (NDTCP) Regulations 2025, focus heavily on anti-money laundering (AML) and institutional stability, but lack explicit safeguards against technology-enabled financial coercion.

To mitigate these risks, the Central Bank of Kenya's (CBK) Consumer Protection Framework must be amended to formally recognize digital financial coercion, such as the forced disclosure of M-Pesa or digital wallet credentials, as a specific form of economic abuse. This amendment should mandate that licensees implement 'safety triggers' for suspicious transaction patterns and establish clear, gender-sensitive reporting and remedy pathways for survivors of domestic and digital financial exploitation.

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. However, 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 behaviors among young men through algorithmic exposure to the manosphere, incel communities, and toxic masculinity content, creating a cohort of current and future workers, managers, and civic leaders with attitudes toward women that are both 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, and its costs should be accounted for accordingly in national budgeting for digital governance and safety infrastructure.

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.
- 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:

- Legal reform.
- Institutional accountability.
- Platform governance.
- Survivor-centred justice.

CHAPTER TWO
REVIEW OF EXISTING LEGAL AND POLICYFRAMEWORKS: GAPS AND REQUIRED AMENDMENTS.

DOMESTIC LEGAL INSTRUMENTS
2.1 THE CONSTITUTION OF KENYA (2010).

2.1.1 Key Constitutional Gap:
While the Constitution provides a robust rights foundation, it does not explicitly recognize digital environments as sites of rights violations. Thus, Kenyan Courts have been called upon to interpret constitutional protections in the digital context on a case-by-case basis, creating inconsistency and uncertainty for survivors seeking redress. There is therefore a compelling case for constitutional-level recognition, of the digital dimensions of the rights guaranteed under Articles 27, 28, and 31 through binding interpretive guidelines issued by the courts, as amending the Constitution is a more complex and longer process.

2.1.2 Why This Matters:
The absence of explicit constitutional recognition of digital rights means that survivors of TFGBV must navigate a patchwork of implied protections, and courts must extrapolate constitutional intent in novel digital contexts. This creates procedural uncertainty and contributes to inconsistent judicial responses.

2.2 THE COMPUTER MISUSE AND CYBERCRIMES ACT (CMCA), 2018 AS AMENDED IN 2024 AND 2025.

The **Computer Misuse and Cybercrimes Act (CMCA) 2018**, as subsequently amended by the Computer Misuse and Cybercrimes (Amendment) Act of 2024 and refined by **the 2025 Amendment Act**, remains Kenya's primary cybercrime statute, and the most directly applicable instrument to Technology-Facilitated Gender-Based Violence.

In its original architecture, Section 27 criminalizes cyber harassment, defined as willfully and repeatedly communicating with a person in a manner that could reasonably be expected to cause that person distress or fear. Section 37 addresses the non-consensual sharing of intimate images.

The 2024 Amendment Act sought to substantially strengthen the Act's deterrent capacity by increasing penalties for cyber-harassment to a maximum of ten years imprisonment or a fine of twenty million Kenya shillings, or both, and by expanding definitions to encompass content that detrimentally affects a person or is likely to cause public panic, and introducing provisions directed at the misuse of social media.

The 2025 Amendment Act further refined these proposals and introduced new offences including SIM-swap fraud under Section 42A and an expanded definition of phishing under Section 30 to incorporate vishing, the use of fraudulent telephone calls to obtain personal information, together with mandatory breach reporting obligations on banks and telecommunications operators relating to Critical Information Infrastructure.

However, the CMCA's current status as the primary instrument of TFGBV enforcement must be understood in light of a significant and ongoing judicial intervention that has materially altered its operational force.

On 22 October 2025, the High Court of Kenya, presided over by Justice Lawrence Mugambi, issued conservatory orders suspending the enforcement of Section 27(1)(b), Section 27(1)(c), and Section 27(2) of the Act, following a constitutional petition filed by the Kenya Human Rights Commission, Reuben Kigame, and others (HCCRPET/E673/2025). The petition challenged the constitutionality of the expanded cyber-harassment provisions on grounds of overbreadth, vagueness of language, and disproportionate infringement on the constitutionally guaranteed right to freedom of expression under Article 33 of the Constitution of Kenya (2010). The conservatory orders remain in force pending a final constitutional determination, the outcome of which will have direct and fundamental consequences for the legal framework governing TFGBV enforcement.

The practical effect of this suspension is that the enhanced penalties, the expanded definition of cyber-harassment, and the provisions criminalizing content likely to cause public panic are currently unenforceable.

The very provisions that the 2024 and 2025 Amendments introduced to close the enforcement gap for TFGBV are precisely those that have been suspended. Prosecutions under the strengthened harassment framework thus cannot proceed, investigations premised on the expanded definitional scope lack statutory foundation, and survivors seeking urgent legal protection against cyber-harassment are returned to the narrower and weaker provisions of the original 2018 Act, for any relief that the criminal justice system can presently provide.

What remains in active force are Section 37 on non-consensual sharing of intimate images, the SIM-swap fraud provisions under Section 42A, the expanded phishing provisions under Section 30, and the Critical Information Infrastructure breach reporting obligations. These provisions are operational and enforceable. However, they do not, individually or collectively, constitute a sufficient statutory basis for comprehensive TFGBV enforcement. The suspension of Section 27 subsections has effectively returned Kenya to a position where the primary tool for prosecuting online harassment of women is a narrower, pre-Amendment provision that predates the recognition of the scale, severity, and gendered nature of TFGBV as it is currently documented.

This judicial intervention is itself a critical gap in the TFGBV legal landscape and must be treated as such in this analysis. It is not merely a procedural complication. It represents a structural vulnerability in the legal architecture, namely the drafting of harassment provisions in terms sufficiently vague to render them constitutionally unsustainable, that will recur unless the underlying legislative design failure is corrected through amendment.

The court's concern with overbreadth and the potential chilling of legitimate expression is not an argument against effective TFGBV legislation. It is an argument for better-drafted, more precisely targeted legislation that can withstand constitutional scrutiny whilst providing robust and enforceable protection. The challenge for legislative reform is to redraft the suspended provisions in a manner that satisfies the constitutional tests of proportionality, necessity, and legality, while maintaining genuine and meaningful protection for survivors of TFGBV.

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, although operational takedown authority remains exercised within the broader statutory and inter-agency framework rather than as an autonomous statutory power.

2.2.1 Identified Gaps:

2.2.1.1 Gender Neutrality and Definitional Failure: The CMCA in its current enforceable form does not define TFGBV as a gender-specific harm. It treats cyber harassment as a generic offence, failing to capture the systemic, gendered, and often coordinated nature of digital violence against women and girls. Multiple state actor respondents who participated in this study confirmed that TFGBV is addressed within their institutions simply as a form of generic GBV amplified by technology, rather than as a distinct, aggravated, and structurally gendered category of harm requiring specialist legal treatment. The suspension of the 2024 and 2025 Amendment provisions has compounded this gap, by removing the most recently updated definitional expansions from the enforceable framework, thus leaving prosecutors reliant on the narrower 2018 language.

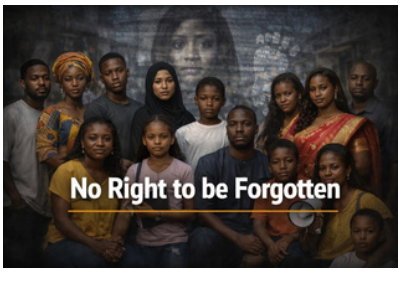
2.2.1.2 The Enforcement Vacuum Created by Judicial Suspension: The suspension of Section 27(1)(b), Section 27(1)(c), and Section 27(2) has created a temporary but critical enforcement vacuum in which the enhanced protections intended to curb TFGBV, are in abeyance pending a final constitutional determination. The duration of this suspension is uncertain, and in the interim, perpetrators of cyber-harassment are effectively insulated from prosecution under the strengthened provisions.

Survivors who reported incidents on the basis of the enhanced framework face the prospect of their cases being unable to proceed on the original charging basis. Prosecutors and investigators are required to work within a framework whose operative boundaries are shifting and legally contested. This uncertainty is itself a structural harm that undermines the deterrent effect of the law, and erodes survivor confidence in the criminal justice system's capacity to respond effectively to TFGBV.

2.2.1.3 Absence of AI-Specific Provisions: Neither the original CMCA nor the 2024 and 2025 Amendments contain any provisions governing AI-generated deepfake sexual imagery, nudify applications, or voice cloning as instruments of TFGBV. This is a major omission as globally, 98% of all online deepfake video content constitutes non-consensual sexual imagery, of which 99% targets women and girls, as documented by Security Hero in 2023 and confirmed by the European Parliamentary Research Service in 2025.

The creation, not merely the sharing, of synthetic intimate imagery remains entirely unpunished under the Act in both its original and amended forms. This is an absolute regulatory void because, the most rapidly growing category of AI-enabled TFGBV has no statutory recognition, no applicable offence, and no penalty framework within Kenya's primary cybercrime statute.

2.2.1.4 No Standalone Non-Consensual Intimate Image Framework: While Section 37 addresses the non-consensual sharing of intimate images and remains in active force, it does not establish a dedicated Non-Consensual Intimate Image (NCII) regime with the specific architecture required for effective survivor protection. There are no emergency takedown orders, no data preservation obligations on platforms pending legal proceedings, no mandatory platform notification requirements, and no interim injunctive relief provisions. As such, survivors of NCII abuse must navigate protracted judicial processes, whilst harmful content continues to circulate, compound trauma, and cause irreversible reputational, professional, and psychological harm. The absence of a rapid remedy framework means that even where a prosecution ultimately succeeds, the survivor's harm has been perpetuated throughout the entire duration of the legal process.



2.2.1.5 No Rapid Takedown or Emergency Relief Mechanism: Neither the current enforceable provisions of the CMCA, nor the suspended provisions, even if they had remained in force, contain a mechanism, empowering courts or regulators to issue immediate takedown orders against online service providers, or social media platforms pending investigation or trial. UNODC's 2025 "Global Strategy on Technology-Facilitated Gender-Based Violence," as presented at the NCII Abuse Summit, New York, specifically identifies the absence of rapid takedown mechanisms as a critical gap that transforms NCII from a single act of abuse into a long-term system of coercion and control. The internet's permanence means that the harm of digital abuse is not bounded by the act of initial publication. It continues, and often escalates, for as long as the content remains accessible. A legal framework without emergency removal powers cannot be an effective framework for survivor protection.
Nevertheless, it worth reiterating that, 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, although operational takedown authority remains exercised within the broader statutory and inter-agency framework rather than as an autonomous statutory power.

2.2.1.6 Constitutional Vulnerability as a Systemic Design Failure: The constitutional challenge that resulted in the October 2025 suspension of Section 27 provisions is not an isolated legal event. It reflects a recurring pattern in Kenyan cybercrime legislation, in which provisions are drafted in broad, vague terms that prioritize expansive deterrence over constitutional precision, and which consequently fail to survive legal challenge. This pattern imposes a systemic cost on TFGBV survivors because, every time a harassment provision is suspended or struck down on constitutional grounds, an enforcement vacuum is created that benefits perpetrators.
The lesson of the October 2025 suspension is not that robust TFGBV legislation is constitutionally impermissible. It is that such legislation must be drafted with scrupulous attention to the constitutional requirements of precision, proportionality, and necessity from the outset, and that drafters must engage comprehensively with the ACHPR Guidelines on Freedom of Expression and Access to Information in Africa, to ensure that the balance between harm prevention and expression protection is properly calibrated in the text of the statute rather than being left to judicial resolution after enactment.

2.2.1.6 No Survivor-Centred Recovery Mechanism: Across both the suspended and the active provisions, the CMCA's architecture is oriented entirely toward the criminal punishment of perpetrators, rather than the immediate protection, recovery, and remediation of survivors. There is no statutory provision for the erasure of harmful digital footprints, no recognition of the right to be forgotten in the digital harm context, and no framework for compensation covering the reputational, professional, psychological, and economic harm caused by TFGBV. This orientation reflects the broader failure of Kenya's criminal justice framework to treat TFGBV as a harm requiring immediate and ongoing survivor-centred intervention, rather than simply a criminal offence awaiting adjudication.

2.2.1.7 Sextortion via Cryptocurrency: The CMCA does not address the financing or facilitation of TFGBV through virtual assets. State actor questionnaire respondents in this study specifically noted that organized criminal networks are increasingly using cryptocurrency to fund cross-border sextortion operations, to receive extortion payments, and to launder the proceeds of TFGBV. This gap cannot be addressed under the current statutory framework. The absence of provisions enabling the tracing, freezing, and forfeiture of cryptocurrency assets connected to TFGBV, means that the financial infrastructure of organized digital sexual violence against women and girls, operates with effective impunity within Kenya's legal architecture.

2.2.2 Required Amendments and Justification:

The constitutional suspension of Section 27 provisions creates both an obligation and an opportunity for legislative reform. The obligation is to redraft the suspended provisions in constitutionally compliant terms, addressing the court's concerns regarding over breadth and vagueness, whilst restoring effective legal protection for TFGBV survivors. The opportunity is to undertake that redrafting as part of a broader, more comprehensive legislative intervention, that addresses all of the structural deficits identified above, rather than simply reinstating the suspended provisions in a minimally amended form.
An amendment to the CMCA should:

- Introduce a comprehensive, standalone TFGBV chapter that incorporates a gender-responsive definition of TFGBV recognizing it as a form of gender-based violence perpetrated, facilitated, or amplified through digital means, drafted in language sufficiently precise to withstand constitutional scrutiny;
- Entail a constitutional compliance protocol for the redrafting of Section 27 that draws on the ACHPR Guidelines on Freedom of Expression, and the proportionality and necessity jurisprudence of the Kenyan courts, to produce cyber harassment provisions that are enforceable and rights-compliant;
- Ensure explicit criminalization of the creation and distribution of AI-generated non-consensual sexual imagery including deepfakes, nudify application outputs, and synthetic intimate content, with offences directed at the act of creation as well as distribution;
- A dedicated NCII offence framework with enhanced penalties that recognize the permanence of digital harm and the severity of reputational, psychological, and economic injury, and that provide for civil as well as criminal remedies;
- A statutory emergency takedown regime empowering courts to issue injunctions requiring online service providers and social media platforms to remove specified content within defined and enforceable timelines pending investigation or trial; a survivor-centred recovery mechanism providing for digital content erasure orders, interim protection orders, and compensation for documented harm including economic loss and reputational injury; and
- Aggravated penalty provisions applicable where TFGBV involves the use of cryptocurrency, cross-border elements, coordinated attacks, or the deliberate targeting of women in public life including journalists, politicians, activists, and human rights defenders.

These amendments are critical for multiple converging reasons including:

- The ongoing suspension of the enhanced harassment provisions means that Kenya currently lacks an effective criminal law response to the most pervasive forms of TFGBV;
- The complete absence of AI-specific provisions means that the fastest-growing category of digital gender-based violence is entirely outside the criminal law;
- The lack of emergency takedown mechanisms means that even the provisions that do exist, cannot provide timely relief to survivors experiencing ongoing harm; and
- The absence of survivor-centred remedies means that even successful prosecutions do not address the continuing injury, that the digital record of abuse inflicts on survivors' lives, careers, and wellbeing.

The proposed amendments are also necessary to bring Kenya into compliance with the Maputo Protocol, ACHPR Resolution 522 on the Protection of Women Against Digital Violence in Africa, the AU Convention on Ending Violence Against Women and Girls adopted in February 2025, and the Budapest Convention on Cybercrime whose accession Kenya has approved and which requires domestic legislative alignment.

Each of these instruments explicitly recognizes digital violence against women as a human rights violation requiring specific, enforceable, and survivor-centred state obligations. Kenya's current enforceable CMCA framework, as assessed against these standards, satisfies none of these requirements adequately. The constitutional suspension of the enhanced provisions has widened rather than narrowed the gap between Kenya's international commitments and its domestic legal reality.

Gap or issue	Current Legal Status	Implication	Recommended Reform
No gender-responsive TFGBV definition	**Not addressed in any version of the Act**	**Generic offences fail to capture systemic digital misogyny; survivors misidentified and cases improperly charged.**	**Introduce standalone TFGBV definition with explicit gender-responsive framing in a new TFGBV chapter of the Act.**
Enhanced harassment provisions suspended	**Section 27(1)(b), (c), and (2) suspended by High Court, October 2025**	**Critical enforcement vacuum; enhanced penalties and expanded definitions unenforceable pending constitutional determination.**	**Redraft suspended provisions with constitutional precision, addressing overbreadth concerns while restoring effective survivor protection.**
No AI or deepfake-specific provisions	**Absent from both original and amended Act**	**Creation of synthetic sexual imagery entirely unpunished; 98% of deepfake content targets women.**	**Criminalize creation and distribution of AI-generated NCII; establish an AI Harm Register with mandatory platform notification obligations.**

Gap or issue	Current Legal Status	Implication	Recommended Reform
No standalone NCII framework	Section 37 active but structurally inadequate	Harmful content circulates throughout legal proceedings; no emergency remedy available to survivors	Establish dedicated NCII offence regime with emergency takedown orders, data preservation obligations, and interim injunctive relief.
No rapid takedown or emergency relief mechanism	Not provided in any provision currently in force	NCII becomes long-term coercion instrument; survivors harmed throughout entire duration of legal process.	Statutory emergency content removal orders enforceable against ISPs and social media platforms within defined timelines.
No survivor compensation framework	Absent from the Act entirely	Survivors bear full reputational, economic, and psychological costs with no statutory restitution.	Introduce restitution orders covering documented economic loss, reputational harm, and psychological injury as civil remedies ancillary to criminal proceedings.
No cryptocurrency or TFGBV provisions	Not addressed in either original or amended Act	Cross-border sextortion financed via virtual assets operates with full impunity.	Criminalize the use of virtual assets to finance or facilitate TFGBV; establish chain analysis obligations and cryptocurrency asset forfeiture provisions.

2.3 THE DATA PROTECTION ACT, 2019

The Data Protection Act (DPA) of 2019 (DPA) establishes a framework for the collection, processing, and storage of personal data and creates the Office of the Data Protection Commissioner as the principal regulatory body. Sections 25 to 31 impose obligations on data controllers and processors, including requirements of lawful processing, data minimization, and purpose limitation. Section 40 grants data subjects a right to erasure of their personal data. The Act provides individuals with rights of access, rectification, and erasure, and empowers the ODPC to investigate complaints, issue enforcement notices, and impose administrative penalties on non-compliant data controllers and processors.

2.3.1 Identified Gaps:

2.3.1.1 The Gender-Neutrality Problem: Functional Blindness in the Face of Gendered Harm: The DPA provides a technically competent and internationally aligned framework for the general safeguarding of personal information. Its gender-neutral drafting is not, in principle, a legislative defect as gender neutrality is the standard approach in data protection law globally, reflecting the universality of the right to privacy, and the aspiration that protective frameworks should apply without discrimination across all persons and all contexts. The problem is not the principle of neutrality. It is the practical consequence of applying a gender-neutral instrument to a category of harm that is, by its nature, structurally gendered, and the functional blindness that results, creates an inability within the Act's architecture to see, name, or respond to the specific, escalatory, and often lethal ways in which personal data is weaponized against women and girls.

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 the same procedural timelines as an unauthorized marketing email, is not a framework calibrated to the reality of the harm it is being asked to address. The Act's uniform lens of privacy loss flattens a spectrum of harm that ranges from administrative inconvenience to existential crisis, and in doing so, it systematically underserves the population that faces the most severe end of that spectrum.

For women and girls, a data breach is rarely only a loss of privacy. It is frequently a precursor to social exclusion, physical violence and professional ruin.

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. These figures, are corroborated by the 2025 Silencing Women Report, 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. This escalating trend underscores a systemic failure in early-warning digital interventions, as many of these physical acts were preceded by documented patterns of online harassment and coercive control.

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.

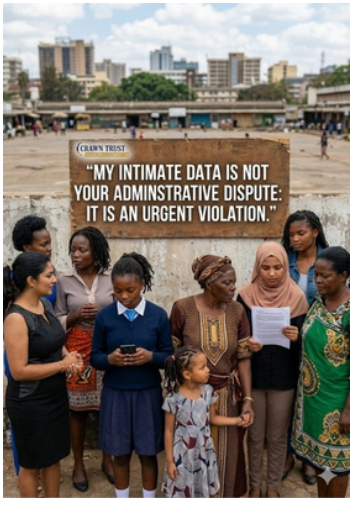
2.3.1.2 Absence of Aggravated Harm Provisions: The Act does not recognize or provide enhanced penalties or accelerated procedures for situations where personal data is specifically leveraged as an instrument of sexual extortion, coercive intimate partner control, sextortion, doxing, or coordinated reputational destruction. This is because all data violations are processed through a uniform enforcement architecture, premised on the notion of privacy loss as a generalized harm, without differentiation based on the severity, intent, or gendered targeting of the violation.

The consequence is that an act of sextortion, in which a perpetrator uses a woman's intimate images or private communications as a tool of ongoing coercion and control over her life, her relationships, her employment, and her physical movements, is treated by the Act with the same procedural weight as a commercial data processor's failure to maintain adequate data security records. This absence of aggravated harm provisions is not a minor technical oversight. It is a structural failure to categorize high-impact, gender-targeted data violations as the serious human rights violations they are.

Without a statutory basis for treating such cases as urgent, the Office of the Data Protection Commissioner (ODPC) has no specific mandate to prioritize TFGBV complaints above routine commercial or administrative data disputes, and no legal architecture through which to deploy enhanced investigative or remedial powers in response to them. As such, cases involving the weaponization of intimate data against individual women are therefore processed, where they are processed at all, within a framework designed for a fundamentally different category of harm, at timelines wholly incompatible with the urgency of the survivor's situation.

2.3.1.3 Incompatibility of Erasure Rights with the Crisis Temporality of Digital Abuse: The right to erasure provided by Section 40 was designed for the administrative context of data correction, and the management of data subjects' ongoing relationships with data controllers and processors. It is a rights-affirming provision within its intended sphere of operation.

In TFGBV contexts, however, it is functionally obsolete. The specific nature of digital abuse, particularly non-consensual intimate image abuse and sextortion, demands near-instantaneous response. The virality of harmful digital content means that the harm it causes compounds exponentially with time, more so because an image shared in an initial act of abuse can be copied, reposted, and permanently embedded across multiple platforms within hours, creating what this analysis elsewhere describes as a Digital Tattoo i.e., a permanent, publicly accessible record of violation that no subsequent erasure order can fully undo.



The standard procedural timelines through which the DPA's erasure rights operate, encompassing the administrative complaint process, the ODPC's investigation and determination, and any subsequent enforcement action against a non-compliant data controller, 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 more efficient administration of the existing framework. It requires a fundamentally different legal instrument, namely an emergency content removal power operative on a crisis timescale, which the DPA does not provide and was never designed to provide. The current reliance on the DPA as a default instrument for data-related TFGBV complaints therefore creates a structural mismatch between the tool available, and the task it is being asked to perform, one that is invisible within the Act's neutral architecture, but acutely felt by every survivor who engages with it.

2.3.1.4 Inadequate Remedies for Data Weaponization and the Enforcement Mandate Gap: The DPA's enforcement mechanisms are primarily administrative rather than survivor-centred, with complaint processes that are slow, procedurally complex, and insufficiently accessible to survivors who are in acute crisis at the point of engagement. The ODPC does not currently possess emergency powers to compel immediate content takedown in cases of severe digital harm. Its investigative and enforcement architecture was calibrated for the commercial and administrative data protection context that the Act was designed to serve, not for the rapid, protective, survivor-oriented intervention that TFGBV cases demand.

The enforcement mandate gap is institutional as well as operational. The ODPC's enabling framework does not include a specific mandate to treat TFGBV-related data violations as urgent human rights emergencies requiring prioritized investigation and accelerated response. Without such a mandate in statute, the Commission is constrained to apply its general enforcement framework uniformly regardless of the severity or gendered character of the violation before it.

TFGBV survivors who approach the ODPC for relief are therefore engaging with an institution whose legal architecture does not equip it to recognize the specific nature of their harm, to prioritize their cases above lower-stakes commercial complaints, or to deploy the rapid, gender-responsive remedial action their circumstances require.

The broader consequence of this enforcement mandate gap is self-perpetuating. The absence of a specific TFGBV mandate within the ODPC means that the Commission is not required to develop gender-responsive operational guidelines for TFGBV cases, to train its staff in the specific dynamics of digital gender-based violence, to maintain disaggregated data on TFGBV complaints as a distinct category, or to report publicly on the adequacy of its response to this category of harm. Without mandate, there is no capacity; without capacity, there is no data; without data, there is no accountability; and without accountability, there is no institutional pressure for reform

.

2.3.1.5 Disconnect from the Criminal Justice System: Survivors of TFGBV involving data violations face a further structural barrier arising from the complete absence of any integrated referral or coordination mechanism between the ODPC and the criminal justice system. As confirmed by multiple stakeholder respondents in this study, survivors are routinely referred between the DCI for criminal investigation and the ODPC for privacy complaints, with neither institution possessing a clear picture of the other's processes, timelines, or evidentiary requirements, and with no one-stop justice mechanism to guide survivors through the intersection of criminal and administrative remedies.

This institutional fragmentation does not merely inconvenience survivors. It constitutes a structural barrier to access to justice that systematically disadvantages the most vulnerable and least resourced complainants, who cannot afford the legal advice necessary to navigate parallel processes simultaneously, and who may disengage from both systems before either delivers any relief.

2.3.1.6 Absence of Explicit Digital Safety Obligations for Platforms: The DPA does not impose explicit safety obligations on social media platforms or online service providers operating in Kenya beyond the general data processing requirements applicable to all data controllers. Platform accountability for TFGBV-enabling conduct, including algorithmic amplification of harmful content, failure to respond to takedown requests, inadequate reporting mechanisms for survivors, and the design of features that facilitate digital coercive control, falls entirely outside the current regulatory scope of the Act.
Platforms operating in Kenya's digital environment are not required by the DPA to implement safety by design principles, to assess the gender-differentiated harm risks of their products and features before deployment, or to demonstrate that their data processing practices do not facilitate or amplify TFGBV.
This absence of platform-specific digital safety obligations represents a significant gap in the regulatory architecture, given that the platforms themselves are the primary medium through which the most pervasive and severe forms of TFGBV are perpetrated and disseminated.

2.3.2 Required Amendments and Justification:

The structural weaknesses identified above require legislative intervention across five distinct dimensions, each of which addresses a specific and documented failure in the DPA's capacity to protect TFGBV survivors.
First, the Act requires the introduction of aggravated harm provisions applicable where personal data is weaponized for gender-based violence or sexual exploitation. These provisions should establish a distinct, elevated category of data violation for TFGBV-related conduct, with enhanced penalties, accelerated investigation timelines, and specific evidentiary standards calibrated to the dynamics of digital gender-based harm. They should explicitly enumerate sextortion, non-consensual intimate image abuse, doxing, digital coercive control, and coordinated reputational destruction as instances of aggravated harm, providing the statutory vocabulary that investigators, prosecutors, and the ODPC currently lack.

Second, the Act requires emergency data erasure and content removal powers exercisable by the ODPC in cases of imminent or ongoing harm, operative on a timescale commensurate with the virality of digital content. These powers should enable the ODPC to issue mandatory removal orders to platforms and data controllers within hours of a complaint being received, supported by interim penalty provisions for non-compliance, and without requiring the survivor to have initiated criminal proceedings or obtained a court order as a precondition. The design of these powers should be explicitly informed by the temporal analysis set out above, because emergency removal is only meaningful if it is fast enough to precede the irreversible embedding of harmful content across multiple platforms.

Third, the Act requires mandatory safety by design obligations on data controllers operating social media platforms, online communication services, and digital dating applications in Kenya. These obligations should require platforms to assess and mitigate the gender-differentiated harm risks of their products and features before deployment, to implement accessible and responsive TFGBV reporting mechanisms, and to demonstrate compliance with safety by design standards as a condition of continued operation within Kenya's regulatory framework.
Fourth, the Act requires explicit statutory integration of the ODPC's mandate with the criminal justice system through a coordination protocol establishing clear referral pathways between the ODPC, the DCI, the ODPP, and Policare for cases involving both criminal and data protection dimensions. This protocol should specify the obligations of each institution at each stage of the referral process, designate case ownership to prevent the survivor being bounced between parallel systems, and establish a single point of contact for TFGBV survivors navigating simultaneous criminal and administrative processes.
Fifth, the Act requires provisions specifically recognizing the heightened sensitivity and vulnerability of data held in intimate partner or domestic contexts where technology is used as a tool of coercive control. These provisions should create an elevated protection category for data within intimate relationships, imposing specific obligations on data controllers whose platforms are foreseeably used for coercive control purposes and establishing survivor rights to emergency account access restoration, device surveillance detection assistance, and digital safety planning support, as data protection remedies in domestic abuse contexts.

These amendments are necessary because privacy violations in TFGBV contexts cause immediate, escalating, and often irreversible harm that cannot wait for standard administrative processes, and because the DPA's current architecture, designed for commercial data protection contexts, is structurally inadequate to address the weaponization of personal data as an instrument of violence against individual women and girls.

The sum of the identified structural weaknesses is that the DPA, as currently drafted and operationalized, provides women and girls who are survivors of data-weaponized TFGBV with a legal instrument that acknowledges their right to privacy in the abstract, whilst failing to deliver meaningful protection in the specific, urgent, and dangerous circumstances in which that right is most severely violated. The proposed amendments are designed to close that gap by transforming the DPA from a passive data governance instrument into an active, survivor-centred component of Kenya's TFGBV protection architecture.

The Sexual Offences Act (SOA) establishes offences relating to sexual violence, including rape, defilement, sexual assault, and indecent acts. It was enacted primarily to address physical acts of sexual violence and reflects the legal understanding of harm that was dominant at the time of its drafting.

2.4.1 Identified Gaps:

2.4.1.1 Physical Contact Requirement: The SOA's 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 outside the Act's definitional scope.

2.4.1.2 Absence of Virtual Sexual Violence Provisions: There is no recognition in the SOA of what legal scholars increasingly describe as virtual or technology-mediated sexual violence, encompassing the creation and distribution of synthetic sexual imagery, non-consensual virtual intimacy, and the use of digital platforms to perpetrate sexual exploitation.

2.4.1.3 No AI-Specific Consent Framework: The Act's consent provisions are anchored in physical interaction and do not provide a framework for assessing consent in the context of AI-generated content that uses a person's likeness without authorization.

2.4.2 Required Amendments and Justification:

The SOA should be amended to extend its definitional framework to cover technology-mediated sexual offences, explicitly including:

- The non-consensual creation or distribution of sexual imagery using a person's likeness, irregardless of whether physical contact occurred;
- virtual sexual harassment causing psychological harm equivalent to that caused by physical sexual assault; and
- sextortion and sexual coercion carried out through digital means.

A technology-facilitated sexual offences schedule should be added as an annex to the Act.

These amendments are critical because the failure to recognize digital sexual violence as equivalent in gravity to physical sexual violence, constitutes a structural gap in women's protection that reflects and perpetuates the legal invisibility of online harm. Survivors of deepfake sexual abuse and NCII suffer profound psychological, reputational, and socio-economic harm that the current Act fails to acknowledge or remedy.

2.5 THE PENAL CODE (CAP. 63)

The Penal Code contains general offences including criminal intimidation, criminal defamation, and malicious communication that may, in some circumstances, be applied to TFGBV conduct. However, constitutional challenges to criminal defamation provisions have significantly limited their utility in TFGBV contexts.

2.5.1 Identified Gaps:

2.5.1.1 Constitutional Vulnerabilities in Defamation Provisions: Criminal defamation provisions have been subject to constitutional challenge and are increasingly regarded as disproportionate restrictions on freedom of expression. Their application in TFGBV contexts creates risks of misuse by state actors and powerful individuals to silence women rather than protect them.

2.5.1.2 Outdated Intimidation Framework: Criminal intimidation provisions predate digital technologies and do not specifically address online threat campaigns, coordinated harassment, or the use of algorithms and automated accounts to intimidate women.

2.6 THE EVIDENCE ACT (CAP. 80) AND DIGITAL EVIDENCE STANDARDS

The admissibility of digital evidence in Kenyan courts remains a significant enforcement barrier. The Evidence Act does not provide comprehensive and technology-specific standards for the collection, preservation, authentication, and presentation of electronic evidence in TFGBV cases. The absence of established protocols for hashing digital evidence, preserving metadata, authenticating screenshots, and handling encrypted communications severely undermines prosecution outcomes. State actor respondents and civil society organizations (CSO) participants confirmed that investigators lack capacity to gather and preserve digital evidence to prosecution standards, that disappearing messages on encrypted platforms prevent evidence collection, and that courts remain uncertain about the admissibility standards for electronically derived evidence in TFGBV cases.

NC4 has authorized a Rapid Reference Guide and Template Charge Sheet under the CMCA 2018 to begin standardizing investigator and prosecutor practice, but this requires legislative underpinning, to ensure evidentiary consistency across all jurisdictions.

2.6.1 Required Reform:

The Evidence Act requires technology-specific amendments establishing mandatory protocols for digital evidence collection and preservation; admissibility standards for electronic evidence including screenshots, call data records, metadata, and geo-location data; provisions for platform-assisted evidence preservation where service providers are required to preserve data pending a court order; and judicial training requirements to ensure consistent application of digital evidentiary standards.

2.7 THE KENYA INFORMATION AND COMMUNICATIONS ACT (KICA), 2013

KICA is the primary instrument regulating the communications sector in Kenya and establishing the mandate of the Communications Authority of Kenya. KICA provides the foundational architecture for the regulation of telecommunications operators, internet service providers, and the broader communications ecosystem within which digital platforms and social media services operate. It confers on the Communications Authority powers to license service providers, set technical standards, and issue directions relating to content standards and service quality. These powers, however, were designed for a broadcasting and telecommunications regulatory context that preceded the emergence of social media platforms as the primary sites of public communication, civic participation, and increasingly gender-based digital violence.

The consequence of this generational mismatch between the statute's design context and the current operational environment is that KICA provides the Communications Authority with the institutional foundation for platform regulation, without equipping it with the specific, enforceable instruments required to compel compliance from global technology companies on matters of TFGBV. The regulatory gap this creates is not simply a gap in coverage, rather it is a gap in leverage, and its consequences for TFGBV survivors are severe and well-documented.

2.7.1 Identified Gaps:

2.7.1.1 The Big Tech Compliance Crisis and the Structural Limits of Administrative Authority: The most concrete and quantifiable evidence of KICA's regulatory inadequacy in the TFGBV context is provided by Google's Global Transparency Report published in February 2026, which records that Google rejected nearly 62% of content removal requests submitted by the Kenyan government in the first half of 2025. While those requests spanned a range of legal grounds including defamation and national security concerns, the rejection rate illuminates a structural problem that applies with particular and catastrophic force to TFGBV cases because, global platforms routinely prioritize their own internally developed Community Guidelines and their politically inflected interpretations of speech protection standards over administrative notices issued by national regulatory bodies, including those issued under Kenyan law.

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, or that the content in question does not violate its Community Guidelines, a survivor of non-consensual intimate image abuse or deepfake sexual exploitation is left in a condition of perpetual, compounding harm, whilst the regulatory system that is supposed to protect her is effectively ignored. The legal authority of the Communications Authority is rendered nominal by the practical capacity of global intermediaries to refuse compliance without facing any consequence that they regard as material. KICA, as currently structured, provides no answer to this refusal.

The problem is structural rather than incidental. 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 the discretion of their own policy teams. This preference reflects both a legal risk calculus, in which platforms regard judicial orders from courts with clear jurisdictional authority as carrying higher legal exposure for non-compliance than regulatory notices, and a political one, in which platforms are sensitive to the reputational consequences of being seen to execute government-directed content removal. The result is that the most effective instrument for compelling platform compliance with TFGBV-related content removal in the current operational environment is a court order issued under enabling legislation that creates unambiguous, enforceable, and financially consequential obligations for non-compliance. KICA does not currently provide that instrument.

2.7.1.2 Absence of Mandatory Gender-Sensitive Content Moderation: KICA does not require platforms operating in Kenya to maintain localized, gender-sensitive content moderation capacity. The platforms that dominate Kenya's digital communication landscape deploy content moderation systems that are predominantly trained on English-language content from Global North contexts, with algorithmic detection systems that are systematically less effective at identifying TFGBV content expressed in Swahili, Sheng, or the cultural and linguistic registers through which gender-based abuse is most commonly perpetrated in Kenyan digital spaces.

The linguistic and cultural specificity of Kenyan TFGBV is therefore systematically invisible to the automated systems nominally responsible for detecting and removing it, and the absence of any legal obligation to maintain localized moderation capacity means that platforms have no regulatory incentive to address this gap.

This is not a hypothetical failure. It is a documented operational reality that contributes directly to the persistence of harmful content targeting Kenyan women and girls on platforms that would likely detect and remove equivalent content expressed in English. The absence of a mandatory localized moderation requirement in KICA means that TFGBV survivors in Kenya receive a structurally inferior level of platform protection, than users in jurisdictions where the platform's primary operating language, aligns with its moderation capabilities.

2.7.1.3 The Absence of Platform Liability for TFGBV-Enabling Conduct: KICA's architecture provides broad safe harbor protections to internet service providers and platforms, insulating them from legal liability for content generated by third-party users on their services. These protections were designed for a context in which platforms were understood as passive conduits for user-generated communication, rather than as active architects of content distribution whose algorithmic systems make consequential decisions about which content is amplified, recommended, and rendered visible to large audiences. That understanding no longer reflects the operational reality of the platforms that dominate Kenya's digital environment, and the safe harbour protections that were reasonable in the former context, have become instruments that effectively immunize platforms from accountability for the TFGBV harm their design choices and algorithmic systems actively facilitate.

There is currently no provision in KICA establishing conditional platform liability for TFGBV-enabling conduct, whether that conduct takes the form of failure to respond to verified takedown requests within defined timelines, algorithmic amplification of content that meets the legal definition of TFGBV, the design of features that demonstrably facilitate digital coercive control, or failure to maintain accessible and responsive TFGBV reporting mechanisms.

Without conditional liability provisions, platforms operating in Kenya have no financial or legal incentive to prioritize the protection of Kenyan TFGBV survivors. Additionally, the Communications Authority has no mechanism through which to impose consequences for non-compliance, that are sufficiently material to alter platform behaviour. And survivors have no direct cause of action against a platform that has refused, or delayed responding to a takedown request whilst their harm compounds.

2.7.1.4 The Absence of a Streamlined Judicial Pathway for Urgent Digital Protection Orders: Because global platforms have established a de facto preference for court orders over administrative requests, the absence of a streamlined, expedited judicial process through which TFGBV survivors can obtain orders that platforms are legally required to recognize and enforce, is a gap with direct daily consequences for survivors seeking relief. The current legal landscape requires a survivor seeking content removal through judicial process to navigate ordinary civil or criminal court procedures, that are not designed for the temporal urgency of digital harm, do not provide for emergency interim orders enforceable against offshore platforms, and do not include mechanisms for confirming platform compliance within defined timescales. By the time an order is obtained through the existing process, the harm it is intended to prevent has in most cases already been fully realized and, in many cases, rendered irreversible by the viral dissemination of the harmful content across multiple platforms and jurisdictions.

KICA does not provide a dedicated judicial pathway for what this analysis terms Urgent Digital Protection Orders i.e., court-issued instruments with mandatory, time-bound compliance obligations enforceable against platforms operating in Kenya regardless of their country of incorporation, carrying automatic financial penalty provisions for non-compliance and supported by clear evidentiary standards, that enable survivors to apply for relief without requiring full legal representation. The absence of this instrument leaves the most urgent category of TFGBV legal need survivors without an adequate legal mechanism, and leaves platforms without a legal obligation that they cannot plausibly refuse to recognize.

Several stakeholder respondents at the February 2026 consultation noted that the Ministry of Interior and National Administration as directed by the National Assembly of Kenya, 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. This is a meaningful administrative development that creates a factual basis for stronger platform accountability obligations. However, the requirement for local presence is currently an administrative direction rather than a statutory obligation, and its enforcement and the obligations that flow from it require legislative underpinning to have binding and consistent effect.

2.7.2 Required Amendments and Justification:

KICA requires fundamental amendment to transform it from a voluntary co-regulation model premised on a broadcasting-era understanding of the communications sector, into a mandatory enforcement framework capable of compelling global technology companies to protect Kenyan TFGBV survivors. This transformation requires reform across four connected dimensions.

First, KICA should be amended to introduce a statutory Urgent Digital Protection Order mechanism, establishing a streamlined, expedited judicial process through which TFGBV survivors can obtain orders with mandatory compliance timelines enforceable against platforms operating in Kenya, regardless of the platform's country of incorporation. These orders should be obtainable on an ex parte basis in cases of acute and ongoing harm, should require compliance within twenty-four hours for the most severe categories of TFGBV content, and should carry automatic and escalating financial penalties for non-compliance, that are calibrated to platform revenue, rather than to fixed sums that global companies can absorb without behavioural change. The instrument of the court order is the form of legal direction, that global platforms have demonstrated they treat as legally serious. Kenyan law should provide TFGBV survivors with access to it, as a matter of urgency.

Second, KICA should be amended to establish conditional platform liability for TFGBV-enabling conduct, replacing the existing broad safe harbour protections with a framework under which a platform loses immunity from liability, where it has received a verified TFGBV complaint or court order and has failed to respond within the mandated timeline, where its algorithmic systems are demonstrated to have amplified TFGBV content, or where the design of its features is found to have facilitated digital coercive control or NCII abuse at scale. Conditional liability provisions create the financial and legal incentive for platform compliance, that purely administrative authority cannot generate, and they reflect the operational reality that modern platforms are not passive conduits, but rather active participants in the distribution of the content that appears on their services.

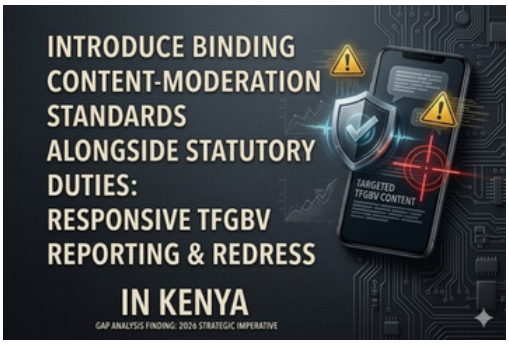
Third, KICA should be amended to impose mandatory localized content moderation requirements on platforms with more than one million Kenyan users, including requirements to maintain moderation capacity in Swahili and the other principal languages in which Kenyan TFGBV is perpetrated, to employ locally based trust and safety personnel with specific responsibility for TFGBV cases, and to demonstrate to the Communications Authority on an annual basis that their content moderation systems are capable of detecting and responding to TFGBV content expressed in the linguistic and cultural registers specific to Kenya's digital environment.

Fourth, KICA should establish mandatory platform transparency and accountability obligations including annual public reporting on TFGBV-related complaints received and actioned, disaggregated by content type, response time, and outcome; data localisation requirements for evidence relevant to TFGBV investigations to ensure that Kenyan law enforcement can access evidential material without requiring mutual legal assistance processes that are too slow to be effective; and financial penalties for non-compliance calibrated to platform revenue, to ensure that the consequence of ignoring Kenyan regulatory authority is material enough to change platform behaviour rather than simply being treated as an acceptable cost of operating in the market.

These amendments are necessary because the current regulatory gap between KICA's administrative authority and the practical leverage required to compel compliance from global technology companies is not a gap that can be closed through more vigorous exercise of existing powers. It is a gap created by the structural design of the statute itself, which was never intended to regulate the entities that now dominate Kenya's digital environment, and which provides those entities with no compelling legal reason to prioritize the protection of Kenyan TFGBV survivors, over their own global policy preferences. The documented 62% rejection rate for Kenyan government content removal requests is not evidence of regulatory failure by the Communications Authority. It is evidence that the regulatory instrument the Authority is currently equipped with is not fit for the purpose to which it is being put, and that the legislative reform required to make it fit is urgent, overdue, and directly consequential for the lives and safety, of the women and girls this analysis is designed to protect.

2.8 THE PROTECTION AGAINST DOMESTIC VIOLENCE ACT, 2015

The Protection Against Domestic Violence Act (PADVA) of 2015 (PADVA) is among the most directly applicable, but least systematically utilized instruments for addressing TFGBV in intimate partner and domestic contexts. The Act defines domestic violence broadly to include psychological, emotional, and economic abuse, intimidation, harassment, and any other conduct that harms, injures, or endangers the health, safety, life, limb, or wellbeing of the complainant. Section 3 explicitly includes harassment and intimidation as forms of domestic violence, and Section 4 creates an obligation on a court to issue a protection order where domestic violence is established or apprehended.



2.8.1 Identified Gaps:

The Act does not explicitly recognize technology as a medium through which domestic violence can be perpetrated. Coercive digital control behaviors documented extensively in this analysis, including the installation of stalkerware on a partner's device, forced password sharing, monitoring of social media communications, location tracking, and the use of intimate images as instruments of coercion or extortion, fall within the spirit of the Act's definition of psychological abuse and intimidation, but are not named within it. This creates interpretive uncertainty for police officers, magistrates, and protection order applicants who may not recognize digital conduct as falling within the PADVA's scope.

The Act also does not establish specific evidentiary standards or procedures for digital evidence in domestic violence proceedings, creating procedural inconsistency when technology-facilitated conduct is presented as evidence of domestic abuse.

There is also no provision directing courts to consider patterns of digital coercive control, as relevant to the assessment of risk when deciding whether to issue, extend, or vary a protection order.

2.8.2 Required Amendments and Justification:

The PADVA should be amended to include an explicit definition of technology-facilitated domestic abuse as a named category within its definition of domestic violence, encompassing non-consensual surveillance via digital means, digital coercive control over financial accounts or communication devices, the use of intimate images or digital content as instruments of intimidation or extortion within domestic relationships, and persistent digital contact or communication designed to cause fear or distress.

The Act should further require courts to consider evidence of technology-facilitated domestic abuse as a relevant factor in protection order applications, and to include specific digital protection provisions within orders issued, including requirements that a respondent refrain from accessing or monitoring a complainant's digital accounts, devices, or communications.

These amendments are critical because the primary site of technology-facilitated coercive control for the majority of women in Kenya is the intimate partner relationship. Stakeholder consultation evidence documented in this analysis confirms that coercive digital control within intimate relationships is systematically under identified, underreported, and under prosecuted precisely because it is not explicitly named as a form of domestic violence in the applicable statute.

The PADVA, being 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.

2.9 THE VICTIM PROTECTION ACT, 2014

The Victim Protection Act (VPA) of 2014 establishes a framework for the recognition, protection, and support of victims of crime in Kenya's criminal justice system. It creates the Victim Protection Board and mandates a series of rights for victims, including the right to dignity and respect, the right to information about the progress of their case, the right to protection from intimidation and secondary victimization, and the right to access support services. Section 9 imposes obligations on criminal justice actors to treat victims with compassion and respect for their dignity.

2.9.1 Identified Gaps:

During stakeholder consultations, a recurring and deeply concerning pattern emerged i.e., survivors of technology-facilitated gender-based violence, particularly those whose intimate images are non-consensually distributed online, experience severe secondary victimization driven by the permanence and virality of the digital record of harm. In numerous cases, survivors reported community ostracism, threats of mob violence, forced displacement from their homes and livelihoods, and the need to relocate for personal safety. These harms persist long after the initial offence, demonstrating that the digital record itself becomes an ongoing site of victimisation.

The VPA does not contain provisions specifically addressing the circumstances of TFGBV survivors, who face a distinctive and aggravated form of secondary victimization arising from the permanent, publicly accessible nature of digital harm. A survivor of non-consensual intimate image abuse or deepfake sexual imagery continues to experience harm throughout the entire period that the content remains accessible online, including during and after the conclusion of any criminal proceedings. The VPA's framework, is designed primarily for the duration of criminal proceedings, and does not address this ongoing, post-trial dimension of victimization.
The Act does not require criminal justice actors to be trained in the specific psychosocial impacts of digital violence, including what is described in the academic literature as Forced Occupational Trauma and Digital Tattoo victimization, the state of perpetual exposure and social harm created by the permanent online record of abuse. There are no provisions requiring referral of TFGBV survivors to specialized digital safety support or to rapid takedown assistance services as part of the victim support framework.

2.9.2 Required Amendments and Justification:

The VPA should be amended to explicitly recognize TFGBV survivors as a protected category requiring specialized protocols, and to impose obligations on the Victim Protection Board to develop and publish TFGBV-specific victim support standards covering trauma-informed digital harm assessment, referral to digital content removal assistance, psychosocial support for ongoing digital victimization, and protection from secondary victimization arising from the digital record of harm. The Board should be required to include digital harm expertise within its operational capacity and to report annually on TFGBV cases processed through the victim support framework.

2.10 THE COUNTER-TRAFFICKING IN PERSONS ACT, 2010

The Counter-Trafficking in Persons Act (CTPA) of 2010 criminalizes trafficking in persons and establishes a framework for victim identification, support, and prosecution of traffickers. Section 3 defines trafficking broadly to encompass the recruitment, transportation, transfer, or receipt of persons through coercion, deception, or abuse of power for purposes of exploitation, including sexual exploitation.

2.10.1 Identified Gaps:

Digital platforms have become primary infrastructure for the recruitment, grooming, and exploitation of trafficking victims, particularly young women and girls. The Act does not contain provisions specifically addressing technology-facilitated trafficking, online recruitment through social media platforms, or the use of digital financial systems to transfer proceeds of trafficking. One state actor questionnaire respondent confirmed reliance on the CTPA in handling TFGBV cases involving financially motivated sexual extortion, reflecting recognition of the overlap between trafficking and digital sexual exploitation, but the Act does not explicitly guide prosecutors or investigators in identifying and charging technology-facilitated trafficking as a distinct category of harm.
The intersection between sextortion and trafficking is particularly important in the Kenyan context. Sextortion operations, including Financially Motivated Sexual Extortion targeting adolescent boys and young men as well as women and girls, have been documented as involving organized criminal networks that use recruitment tactics, platform-based grooming, and coercive digital control in ways that may meet the CTPA's definition of trafficking, but are not currently recognized or charged as such.

2.10.2 Required Amendments and Justification:

The CTPA should be amended to introduce explicit provisions on technology-facilitated trafficking encompassing online recruitment, digital grooming, and platform-mediated exploitation, and to establish coordination obligations between the Counter-Trafficking in Persons Advisory Committee and NC4, the DCI Cybercrime Unit, and the ODPC for cases involving digital elements.
Prosecution guidelines should specifically address the evidential overlap between sextortion and trafficking charges, to ensure that the most serious applicable charge is consistently preferred.

2.11 THE CHILDREN ACT, 2022

The Children Act, 2022, which revises and consolidates Kenya's child protection framework, establishes the rights of children and obligations for their protection from exploitation, abuse, and neglect. Section 23 protects children from all forms of abuse, and Section 24 imposes obligations on the state and duty-bearers to prevent, investigate, and respond to child abuse. The National Council for Children's Services administers the Act's protective framework.

2.11.1 Identified Gaps:

The Children Act does not contain specific provisions addressing technology-facilitated abuse of children, including online grooming, exposure to harmful digital content through algorithmic recommendation, digital peer abuse including the circulation of intimate images between minors, or the exploitation of children through digital platforms by adult predators.

The Act's definition of abuse does not explicitly reference digital or technology-mediated conduct, creating interpretive uncertainty equivalent to that identified in the Protection Against Domestic Violence Act.

The Act does not address the specific harms arising from the deployment of AI-driven digital learning tools and behavioral data collection systems in Kenyan schools, under the Competency Based Curriculum, or the obligations of educational institutions to protect children's digital safety and data sovereignty within school environments. There is no provision establishing parental rights to information, about how their children's behavioral and learning data is collected and used by the digital platforms operating within the educational system.

2.11.2 Required Amendments and Justification:

The Children Act should be amended to explicitly recognize technology-facilitated abuse of children as a specific and named category within its definition of child abuse; to impose obligations on digital platform operators whose services are directed at or foreseeably used by children to implement child safety measures 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 principles of the Convention on the Rights of the Child to which Kenya is a party.

2.12 THE EMPLOYMENT ACT, 2007

The Employment Act of 2007 regulates employment relationships in Kenya and includes provisions relating to sexual harassment in the workplace under Section 6. Section 6 defines sexual harassment to include unwelcome conduct of a sexual nature that has the purpose or effect of violating an employee's dignity or creating a hostile, intimidating, or humiliating work environment, and imposes obligations on employers of twenty or more employees to establish a sexual harassment policy.

2.12.1 Identified Gaps:

Section 6 of the Employment Act was drafted before the emergence of digital communications as the primary medium of professional interaction. It does not explicitly recognize digital workplace harassment as a form of sexual harassment, leaving a significant enforcement gap for the behaviors documented at the CRAWN Trust February 2026 stakeholder consultation, including sexual messages transmitted via professional messaging platforms, late-night video call demands, professional advancement conditioned on private digital communications, and the creation of hostile digital work environments through persistent online targeting of female colleagues.

Drawing from the 2025 UNESCO-FeCoMo High-Level Roundtable, the Kenya Editors' Guild has formally recognized the digital sphere as an inseparable extension of the professional workspace. This position affirms that journalists and media workers are entitled to the full protection of labour rights and occupational safety standards while performing their duties online.

Despite this professional affirmation, a significant statutory gap remains. The Employment Act (2007) and the Occupational Safety and Health Act (OSHA) currently fail to define 'digital professional environments' or recognize technology-facilitated gender-based violence (TFGBV) as a workplace hazard. Consequently, while the Kenya Editors Guild mandates an institutional duty of care, survivors lack a clear statutory pathway under the Employment Act to hold employers accountable for failing to mitigate digital harms, or provide 'digital PPE' (security tools and legal support).

Employers are not currently required to include digital conduct in their sexual harassment policies, or to establish reporting mechanisms for digital workplace harassment. The institutional framework for addressing workplace sexual harassment, including the National Labour Relations Commission, has no specific guidance on or capacity for handling technology-facilitated workplace harassment complaints.

2.12.2 Required Amendments and Justification:

Section 6 of the Employment Act should be amended to explicitly extend its definition of sexual harassment to include unwelcome conduct of a sexual nature transmitted through digital communication platforms, messaging applications, email, social media, or any other electronic medium arising from or related to an employment relationship.

Employers should be required to include specific provisions on digital conduct, reporting mechanisms for digital harassment, and investigation procedures for electronically transmitted harassment complaints, within their statutory sexual harassment policies.

These amendments are essential because workplace digital harassment is systematically dismissed as ordinary workplace conflict, rather than identified and addressed as the labour rights violation it constitutes, leaving affected workers, who are disproportionately women, without remedy and employers without accountability.

2.13 THE NATIONAL COHESION AND INTEGRATION ACT, 2008

The National Cohesion and Integration Act (NCIA) of 2008 prohibits hate speech and discrimination on grounds including ethnicity and other group characteristics, establishes the National Cohesion and Integration Commission (NCIC), and creates criminal liability for the promotion of hatred, discrimination, and ethnic tension. Sections 13 and 62 establish offences relating to hate speech and discriminatory practices.

2.13.1 Identified Gaps:

The NCIA does not explicitly address gender as a protected characteristic for the purposes of its hate speech provisions, and its drafting reflects a primary concern with ethnic and community-based incitement to violence rather than gendered hate speech.

Coordinated online campaigns targeting women because of their gender, political activity, or public visibility, including the manosphere-driven campaigns documented in this analysis, may not meet the NCIA's definitional threshold for hate speech as currently drafted.

The NCIC's mandate and operational focus has historically been directed at ethnic and political conflict rather than at gender-based online hate speech, leaving a gap in institutional accountability for the producers of coordinated misogynistic digital attacks.

In Kenya's pre-election period, the intersection of gendered hate speech and political incitement is acute. AI-generated disinformation targeting women candidates and combining gendered abuse with ethnic or political incitement may simultaneously engage the NCIA and the CMCA without either statute providing a complete legal framework for prosecution.

2.13.2 Required Amendments and Justification:

The NCIA should be amended to explicitly include gender as a protected characteristic within its hate speech and discrimination provisions, and to extend its definition of hate speech to encompass coordinated digital campaigns designed to intimidate, silence, or incite harm against individuals because of their gender or gender identity.

The NCIC should be required to publish annual monitoring data on gender-based online hate speech, and to coordinate with the Communications Authority and NC4, on enforcement action against digital content constituting gendered incitement.

2.14 THE MEDIA COUNCIL ACT, 2013

The Media Council Act of 2013 establishes the Media Council of Kenya and provides a framework for media regulation, including standards of professional practice, the accreditation of journalists, and mechanisms for addressing complaints against media practitioners. Section 21 imposes obligations on the Media Council to promote the safety of journalists.

2.14.1 Identified Gaps:

The Media Council Act does not contain provisions specifically addressing the digital safety of women journalists, or the institutional obligations of media houses to protect their employees from technology-facilitated harm, arising from their professional activities.

The Act's professional standards framework predates the emergence of coordinated digital attacks against journalists, as a systematic tool of press intimidation. As documented in this analysis, women journalists in Kenya face what the International Association of Women in Radio and Television describes as a permanent hostile digital work environment arising from their professional visibility, with consequences including Forced Occupational Trauma, self-censorship, and abandonment of accountability beats.

The Media Council's current framework has no mechanism for recognizing, recording, or responding to this as a professional safety issue.

2.14.2 Required Amendments and Justification:

The Media Council Act should be amended to impose explicit obligations on media organizations to establish digital safety policies and support mechanisms for journalists facing TFGBV; to require the Media Council to publish annual data on digital harassment reported by journalists disaggregated by gender; and to recognize digital safety as a component of the professional standards framework applicable to media practitioners.

The Council should be required to coordinate with the National Computer and Cybercrimes Coordination Committee (NC4)and the DCI on cases involving criminal threats to journalists through digital means.

2.15 THE NATIONAL GENDER AND EQUALITY COMMISSION ACT, 2011

The National Gender and Equality Commission Act of 2011 establishes the National Gender and Equality Commission (NGEC) as a constitutional commission under Article 59 of the Constitution, with a mandate to promote gender equality and freedom from discrimination, monitor, facilitate, and advise on the integration of the principles of gender equality across all areas of public and private life, and receive and investigate complaints related to gender-based discrimination.

2.15.1 Identified Gaps:

The NGEC's statutory mandate does not explicitly include a technology-specific dimension, and the Commission has no legislated obligation to monitor, investigate, or report on TFGBV as a dimension of gender equality in Kenya. The NGEC questionnaire respondent in this study identified insufficient reliable data on TFGBV as a critical governance gap, confirming that the Commission's current operational framework does not generate the systematic, disaggregated data necessary to track TFGBV as a policy priority.

Additionally, there is no statutory obligation for other state institutions to report TFGBV data to the NGEC, thus limiting the Commission's ability to exercise its monitoring mandate effectively in the digital sphere.

2.15.2 Required Amendments and Justification:

The NGEC Act should be amended to explicitly include TFGBV within the Commission's monitoring and investigation mandate; to empower the NGEC to require state and non-state actors to submit disaggregated TFGBV data as part of the Commission's gender equality monitoring function; and to require the NGEC to publish a biennial report specifically on TFGBV prevalence, institutional response, and survivor access to justice in Kenya.

These amendments would institutionalize the data collection and accountability function that is currently absent from Kenya's TFGBV governance architecture, and provide the evidential foundation for evidence-based legislative and policy reform on an ongoing basis.

2.16 THE ARTIFICIAL INTELLIGENCE BILL, 2026: A CRITICAL ASSESSMENT.

The Artificial Intelligence Bill, 2026, sponsored by Nominated Senator Karen Nyamu and currently before the Senate, represents Kenya's most significant legislative attempt to date to govern the development, deployment, and use of artificial intelligence. Its animating concerns are directly relevant to this gap analysis because, the Bill criminalizes deepfake-generated content, adopts a risk-based regulatory model aligned with the European Union's Artificial Intelligence Act, and requires the Advisory Committee on AI to be gender-balanced.

The fact that the Bill has its origins, in part, in the documented experience of a female politician subjected to AI-generated harassment places TFGBV at the centre of its political rationale. 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 development.

However, in its current form, the Bill is not viable as an effective instrument for addressing TFGBV and requires significant amendment before enactment. Its most critical structural weakness is the proposal to establish three entirely new regulatory bodies, an AI Commissioner, an AI Authority, and an Advisory Council, in a governance landscape that already operates an Office of the Data Protection Commissioner with statutory authority over automated decision-making and a Communications Authority regulating digital content. This architecture creates parallel regulatory structures whose jurisdictional boundaries are undefined, and whose interaction with existing institutions such as NC4 and the DCI is unaddressed.

For a TFGBV survivor who has experienced AI-generated intimate image abuse, the practical consequence could be a requirement to navigate three separate oversight bodies simultaneously, with no integrated referral pathway between them, compounding precisely the institutional fragmentation that this analysis identifies as one of the six foundational failures in Kenya's current TFGBV response.

The Bill also lacks gender-specific provisions despite its origins because the risk classification framework does not identify AI systems generating non-consensual sexual imagery as inherently prohibited risk applications, and there are no provisions addressing model poisoning, prompt injection attacks on survivor support systems, or the particular compliance burden that full audit trail requirements would impose on Kenya's developer ecosystem, the majority of whom adapt pre-trained open-source models, rather than building AI from scratch.

Despite these significant shortcomings, the Bill provides a necessary and valuable foundation for what must now become an urgent national conversation about AI governance.

Kenya cannot afford to wait for a perfect Bill before beginning the legislative process, and the framework proposed, including risk classification, regulatory sandboxes, transparency requirements, and criminal penalties for misuse, contains the building blocks of an effective regime.

What is required is targeted amendment rather than rejection because designating the AI Commissioner as a coordinating body operating through existing institutional mandates rather than alongside them; explicitly classifying AI systems generating non-consensual sexual imagery as prohibited risk applications; introducing dedicated children's AI protection provisions to address the harms currently occurring in Kenyan classrooms and on children's devices; incorporating electoral AI disinformation provisions responsive to the 2027 General Election risk; and calibrating compliance obligations to distinguish between developers, deployers, and operators of pre-trained models. 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.

REGIONAL AND INTERNATIONAL FRAMEWORKS: ALIGNMENT AND IMPLEMENTATION GAPS.

Kenya has ratified or committed to a range of regional and international frameworks that impose explicit obligations with respect to TFGBV, yet implementation remains materially incomplete across all of them. The following analysis maps Kenya's commitments and the specific gaps between formal accession and domestic legal effect.

2.17 THE CONSTITUTION OF KENYA AND THE AFRICAN CHARTER ON HUMAN AND PEOPLES' RIGHTS (1981)

The Maputo Protocol, which is addressed in section 2.18 below, is a protocol to the African Charter on Human and Peoples' Rights rather than a freestanding instrument. The Charter itself, to which Kenya is a party, imposes direct and binding obligations relevant to TFGBV that extend beyond those in the Maputo Protocol, and require specific acknowledgment. Article 2 prohibits discrimination of any kind including on the basis of sex. Article 3 guarantees equality before the law. Article 4 protects the right to life and integrity of the person. Article 5 prohibits degrading treatment.

The African Commission on Human and Peoples' Rights, which monitors Charter compliance, has through its Guidelines on Freedom of Expression and Access to Information in Africa (2019) affirmed that state obligations to prevent and remedy online violence against women are consistent with, and not in conflict with, obligations to protect freedom of expression. This interpretive guidance is directly relevant to the concern expressed during the stakeholder consultation that TFGBV enforcement measures risk becoming instruments of censorship. The ACHPR Guidelines provide the authoritative regional framework for navigating the tension between enforcement and free expression protection, and should be explicitly referenced in the legislative drafting process for any standalone TFGBV statute.

2.18 THE MAPUTO PROTOCOL (PROTOCOL TO THE AFRICAN CHARTER ON HUMAN AND PEOPLES' RIGHTS ON THE RIGHTS OF WOMEN IN AFRICA)

Articles 3 and 4 of the Maputo Protocol guarantee women's rights to dignity, life, and integrity. The Protocol's protection extends to digital environments through ACHPR Resolution 522 on the Protection of Women Against Digital Violence in Africa of 2022, which explicitly recognizes digital violence as a human rights violation and affirms state obligations to prevent, investigate, punish, and provide remedies. ACHPR Resolution 522 calls on states to adopt specific legislation on digital violence against women, establish dedicated institutional mechanisms, and ensure access to redress. Kenya's current framework satisfies none of these requirements comprehensively, exposing Kenya to criticism in treaty body reviews, and constituting a failure to meet the obligations freely assumed under international law.

2.19 THE AU CONVENTION ON ENDING VIOLENCE AGAINST WOMEN AND GIRLS (ADOPTED FEBRUARY 2025)

The AU Convention on Ending Violence Against Women and Girls, adopted in February 2025, is the first regional treaty to expressly address violence within cyberspace. It establishes binding obligations on AU member states to adopt legislation, policies, and institutional mechanisms specifically addressing technology-facilitated violence.

Kenya's accession to, and domestic implementation of this Convention, should be treated as a priority legislative reform milestone, as its provisions represent the most current and specific continental articulation of the obligations that the CMCA, Data Protection Act, and Sexual Offences Act amendments recommended in this analysis are designed to fulfill.

2.20 CEDAW AND GENERAL RECOMMENDATION NO. 35 (2017)

CEDAW General Recommendation No. 35 of 2017 recognizes online and technology-facilitated violence against women as a form of gender-based discrimination requiring state action. CEDAW's monitoring mechanisms have consistently called on Kenya to strengthen its legal framework and enforcement capacity.

The General Recommendation specifically addresses the obligation of states to ensure that laws on TFGBV are accessible, effective, and enforced, and that survivors have access to legal aid, psychosocial support, and remedies without facing secondary victimization. These specific obligations map directly onto the gaps identified in Kenya's VPA, Employment Act, and CMCA frameworks as analysed above.

2.21 THE BUDAPEST CONVENTION ON CYBERCRIME

Kenya has approved accession to the Budapest Convention on Cybercrime, which will facilitate cross-border investigation and prosecution of cybercrime including TFGBV. Operationalization of the Convention's mutual legal assistance and extradition frameworks is essential to address the transnational nature of digital abuse, including the cross-border sextortion operations funded via cryptocurrency identified by state actor respondents in this analysis. Domestic legislative alignment with the Budapest Convention's requirements for electronic evidence preservation, mutual legal assistance procedures, and twenty-four-seven contact point mechanisms will require targeted amendments to the Evidence Act and the CMCA as recommended in Sections 2.2 and 2.6 of this analysis.

2.22 THE MALABO CONVENTION (AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION)

Kenya has approved accession to the Malabo Convention, providing a continental framework for cybercrime governance and data protection. Full operationalization will require domestic legislative alignment, including ensuring that the Data Protection Act's provisions meet the Malabo Convention's standards for data protection, and that Kenya's cybercrime enforcement architecture, including NC4's mandate and the DCI's digital forensic capacity, meets the Convention's institutional requirements.

The Malabo Convention's personal data protection provisions provide additional support for the DPA amendments recommended in Section 2.3 of this analysis, situating them within a binding continental framework rather than relying solely on domestic policy arguments.

2.23 ILO CONVENTION 190 ON VIOLENCE AND HARASSMENT (2019)

ILO Convention 190, the Violence and Harassment Convention of 2019, is the first international labour standard to specifically address violence and harassment in the world of work, including workplace sexual harassment and gender-based violence occurring in the context of employment.

The Convention defines violence and harassment to include a range of unacceptable behaviors and practices that aim at, result in, or are likely to result in physical, psychological, sexual, or economic harm, and explicitly recognizes that violence and harassment can occur through work-related communications enabled by technology.

Kenya has not yet ratified Convention 190, which represents both a gap in its international accountability framework and a critical advocacy opportunity.

The Convention's companion Recommendation 206 specifically addresses the need for policies on gender-based violence and harassment in the workplace, that encompass digital communications, a standard that Kenya's current Employment Act framework does not meet as analysed in Section 2.12 above. Ratification of Convention 190 would create a binding international obligation to amend the Employment Act in the manner recommended in this analysis, and would align Kenya's labour rights framework with contemporary global standards on digital workplace harassment. Ratification should be recommended as a priority advocacy target in the Strategic Policy Brief emerging from this analysis.

2.24 THE UN DECLARATION ON THE ELIMINATION OF VIOLENCE AGAINST WOMEN (1993) AND THE UN SPECIAL RAPPORTEUR FRAMEWORK

The UN Declaration on the Elimination of Violence Against Women of 1993 remains the foundational international instrument defining state obligations with respect to violence against women, and establishing the principle that violence against women constitutes a violation of women's human rights and fundamental freedoms.
The Declaration's definition encompasses psychological harm and includes violence perpetrated or condoned by the state, as well as by private actors, a principle that has direct relevance to TFGBV perpetrated through private digital platforms, that the state has failed to regulate.

The UN Special Rapporteur on Violence Against Women has issued specific reports and country mission observations relevant to Kenya, including guidance on technology-facilitated violence that sets out the evidentiary standards, legislative elements, and institutional mechanisms required for an adequate state response.

The Special Rapporteur's reports constitute highly persuasive international guidance that should inform the legislative recommendations emerging from this analysis, and be cited in the Strategic Policy Brief to strengthen the case for reform before parliamentary and executive audiences.

2.25 THE UN CONVENTION ON THE RIGHTS OF THE CHILD (1989) AND GENERAL COMMENT NO. 25 (2021) ON CHILDREN'S RIGHTS IN RELATION TO THE DIGITAL ENVIRONMENT.

Kenya is a party to the UN Convention on the Rights of the Child (CRC) and is bound by Article 34, which requires states to protect children from all forms of sexual exploitation and sexual abuse, and Article 36, which protects children against all other forms of exploitation prejudicial to their welfare.

General Comment No. 25 of 2021, issued by the Committee on the Rights of the Child, provides comprehensive guidance on the application of CRC obligations in digital environments. It explicitly addresses children's right to be protected from digital violence, online grooming and sexual exploitation, algorithmic profiling of children, and the deployment of AI systems in ways that harm children's development and wellbeing.

The General Comment establishes that states must conduct child rights impact assessments before deploying digital services that affect children, must regulate private sector actors to protect children in digital environments, and must ensure that children have effective access to remedy when digital rights violations occur. It provides the authoritative international legal foundation for the child-specific legislative amendments recommended in Sections 2.11 of this analysis and for the children's AI protection provisions recommended as well.
Kenya's domestic legal framework, including the Children Act and the nascent AI Bill, must be assessed against General Comment No. 25 as the applicable international standard.

2.26 THE SUSTAINABLE DEVELOPMENT GOALS AND GENDER ACCOUNTABILITY MECHANISMS

The UN Sustainable Development Goals, to which Kenya has committed as part of its Vision 2030 and bottom-up development agenda, provide an accountability framework that is often more politically accessible than human rights instruments in engaging finance, planning, and development ministries.
SDG 5 on gender equality specifically targets the elimination of all forms of violence against all women and girls in public and private spheres, including trafficking and sexual and other types of exploitation, and calls for the use of enabling technology to promote women's empowerment. SDG 16 on peaceful, just, and inclusive institutions calls for significantly reducing all forms of violence and ensuring equal access to justice for all.

Kenya's Voluntary National Review submissions to the UN High-Level Political Forum on Sustainable Development, provide an existing accountability mechanism through which TFGBV governance progress can be tracked and reported internationally. Framing the recommendations emerging from this analysis within the SDG accountability architecture enables engagement with Treasury and planning ministries whose primary accountability language is development rather than human rights, and may therefore be more effective in securing the budgetary allocations necessary to implement the institutional reforms recommended in this report.

2.27 THE AFRICAN UNION AGENDA 2063 AND THE DIGITAL TRANSFORMATION STRATEGY FOR AFRICA (2020 TO 2030)

The African Union's Agenda 2063, to which Kenya is committed as a founding member state, explicitly includes gender equality as a foundational development principle and Aspiration seven, which calls for a continent where the full potential of women and youth is realized.
The Digital Transformation Strategy for Africa of 2020 to 2030 sets out the AU's framework for digital infrastructure development, cybersecurity, and digital inclusion, including specific commitments to ensuring that digital transformation benefits women and marginalized groups, rather than exacerbating existing inequalities.
These frameworks provide the development policy context within which Kenya's TFGBV governance must be situated. The argument that addressing TFGBV is a precondition of realizing the digital inclusion and gender equality commitments of both Agenda 2063 and the Digital Transformation Strategy, is a powerful advocacy framing for engaging multilateral development partners and continental institutions invested in meeting AU development commitments.

The gap between Kenya's TFGBV governance architecture and the standards required to realize digital inclusion for women and girls is not only a human rights failure. It is a development failure that undermines Kenya's commitments at the highest levels of continental and global governance, and exposes the country to reputational and accountability consequences that extend well beyond the human rights review cycle.

2.28 THE COUNCIL OF EUROPE ISTANBUL CONVENTION (2011) AS A COMPARATIVE BENCHMARK

Kenya is not a party to the Istanbul Convention on Preventing and Combating Violence Against Women and Domestic Violence, which is a Council of Europe instrument.

However, the Istanbul Convention has been widely recognized as the international gold standard for comprehensive legislative frameworks addressing violence against women and has been explicitly referenced by UN treaty bodies, the ACHPR, and regional policy frameworks as a benchmark for adequate state responses.

Article 17 requires parties to encourage the media and private sector to develop self-regulatory standards to prevent violence against women, directly relevant to the platform accountability recommendations in this analysis. Article 50 establishes obligations for law enforcement to respond immediately, and appropriately to cases of violence against women, relevant to the police response reforms recommended in Section 7 of this report.

Its inclusion as a comparative reference standard in the legal mapping, clearly flagged as persuasive rather than binding, serves a specific advocacy function because, it allows drafters and parliamentary advocates in Kenya to calibrate the ambition of proposed reforms, against the most comprehensive international benchmark, and to anticipate and respond to arguments that the proposed measures are disproportionate, or unprecedented. This framing strengthens rather than overstates Kenya's reform obligations.

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 Lead Consultant, Mutheu Nyagah Khimulu, providing an overview of the TFGBV landscape in Kenya, followed by facilitated discussion that generated rich, 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 stakeholder contributions are treated as confidential. Participants are not identified by name in this report; their contributions are attributed to their institutional roles or areas of expertise only.

This chapter synthesizes the principal thematic issues raised, identifies patterns and convergences, and reflects the evidence generated against the broader findings of the gap analysis.

3.1 THE EXPANDING TYPOLOGY OF TFGBV: BEYOND CONVENTIONAL CATEGORIES.

A consistent theme across the consultation was the breadth and evolving nature of TFGBV beyond the forms most commonly captured in legal and policy discourse. Practitioners from across the institutional and civil society spectrum, documented forms of TFGBV that remain largely invisible in existing legal frameworks, each representing 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, encompassing 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 working at the grassroots level, 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, noting that this form of harm shapes women's freedom, and political participation in ways that are both real, and insufficiently acknowledged by existing legal definitions.

3.1.2 Workplace Digital Harassment:

A representative from a civil society organization focused on media and communications, highlighted workplace digital harassment as a pervasive and systematically dismissed form of TFGBV, 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 but is rarely recognized, or prosecuted as such, reflecting a significant gap in institutional awareness and enforcement.

The Kenya Editors' Guild has publicly affirmed that the digital workplace constitutes a full extension of the professional workspace, and that constitutional labour rights protections apply in their entirety to digital professional environments, a position the statutory text of the Employment Act does not yet reflect.

3.1.3 Cancel Culture as Political Censorship:

A practitioner working in democratic governance and civic participation, identified the weaponization of coordinated cancel culture campaigns against women in political circles and public life as an underrated form of TFGBV.

These campaigns are designed to delegitimize women's credibility, and drive them from digital platforms, functioning as political censorship with material consequences for 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:

A practitioner in civic society, raised the surveillance of journalists and activists through social media monitoring 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, with the observation that the system could morph into a tool to track citizens' movements or resources if deployed without robust privacy safeguards. This forward-looking concern demands proactive regulatory attention and explicit privacy provisions, in the system's design architecture before deployment.

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.

Adolescent girls remain the most disproportionately affected population in these educational digital contexts, a finding consistent with research published by the United Nations Population Fund on TFGBV in Kenyan higher learning institutions, which found that 64.4% of female students surveyed had personally experienced online violence, nearly double the rate of their male peers.

3.1.6 Intimate Image Abuse and the Lethal Continuum:

A practitioner working 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. This account illustrates in the starkest possible terms the lethal continuum between TFGBV and physical femicide that underpins the urgency of this analysis, and that is further substantiated by the 579 femicide cases recorded in Kenya in 2024, many preceded by digital threats and stalking, as documented by UNESCO and national police data.

The perpetrator in the coast case was subsequently arrested and charged, but a life had already been lost. 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 specific and 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.

The combination of deepfake technology with Kenya's mobile penetration rate of 149.4%, as recorded by the Communications Authority of Kenya, and the limited digital literacy of many voters, creates conditions in which AI-enabled electoral TFGBV could materially influence political outcomes and silence women candidates.

3.2 SYSTEMIC INSTITUTIONAL AND LEGAL CHALLENGES.

Participants consistently identified a cluster of systemic challenges that undermine effective prevention, reporting, investigation, and prosecution of TFGBV across all sectors and levels of government. This section will delve into the main concerns raised.

3.2.1 The Absence of a Standalone TFGBV Definition in Law:

Practitioners across the media, civil society, and legal sectors articulated 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 rather the predictable and recurring consequence of a definitional vacuum that cascades through every stage of the justice chain.

Multiple respondents across both the consultation and the key informant questionnaire streams confirmed this assessment independently, underscoring that the absence of a dedicated TFGBV legal definition constitutes the single most foundational gap in Kenya's current response architecture.

3.2.2 Digital Evidence Collection Failures:

The consultation documented evidence failures at multiple points in the investigative and prosecutorial chain. 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.

A practitioner in civil society focused on women's rights, identified forensic evidence requirements as a practical difficulty in charging TFGBV cases, noting that survivors often do not know how or where to report, and that institutions are uncertain about applicable charges.

These observations align with the evidentiary gaps identified in the analysis of the Evidence Act in Chapter 2 of this report, and with the **KICTANet research on the existing legal framework addressing TFGBV in Kenya**.

3.2.3 Public Awareness Deficits:

A gender officer from a county government and a civil society representative working in community development, both identified limited public awareness of TFGBV, and of available legal frameworks as a primary barrier.

In the assessment of these practitioners, 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 from development and civil society organizations, called for structured engagement with technology platforms to ensure accountability, faster content removal, and transparent response mechanisms.

It was noted that even where laws exist, enforcement is weak due to training, resource, and political will deficits, and that the cross-border nature of online violence creates jurisdictional barriers to the prosecution of offshore perpetrators.

Two social media platforms, 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 OGBV Tracker was shared during the stakeholder consultation as a practical tool for monitoring and recording TFGBV cases that could be leveraged for national data aggregation.

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 review, and with the broader evidence base compiled in this analysis.

3.3 GOVERNMENT CAPACITY AND ONGOING INITIATIVES.

A representative from a national cybercrime coordination institution provided important testimony regarding the government's growing institutional capacity. The National Computer and Cybercrimes Coordination Committee (NC4) is in the advanced stages of developing a CMCA 2018 Rapid Reference Guide and Template Charge Sheet, which will be available through the NC4 website, where one can find other vital information.

The Rapid Reference Guide and Template Charge Sheet will standardize how investigators and prosecutors handle digital threats including TFGBV. The Ministry of Interior and National Administration has also 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 and Malabo Conventions to allow cross-border investigation and is operationalizing cyber desks to enhance reporting visibility.

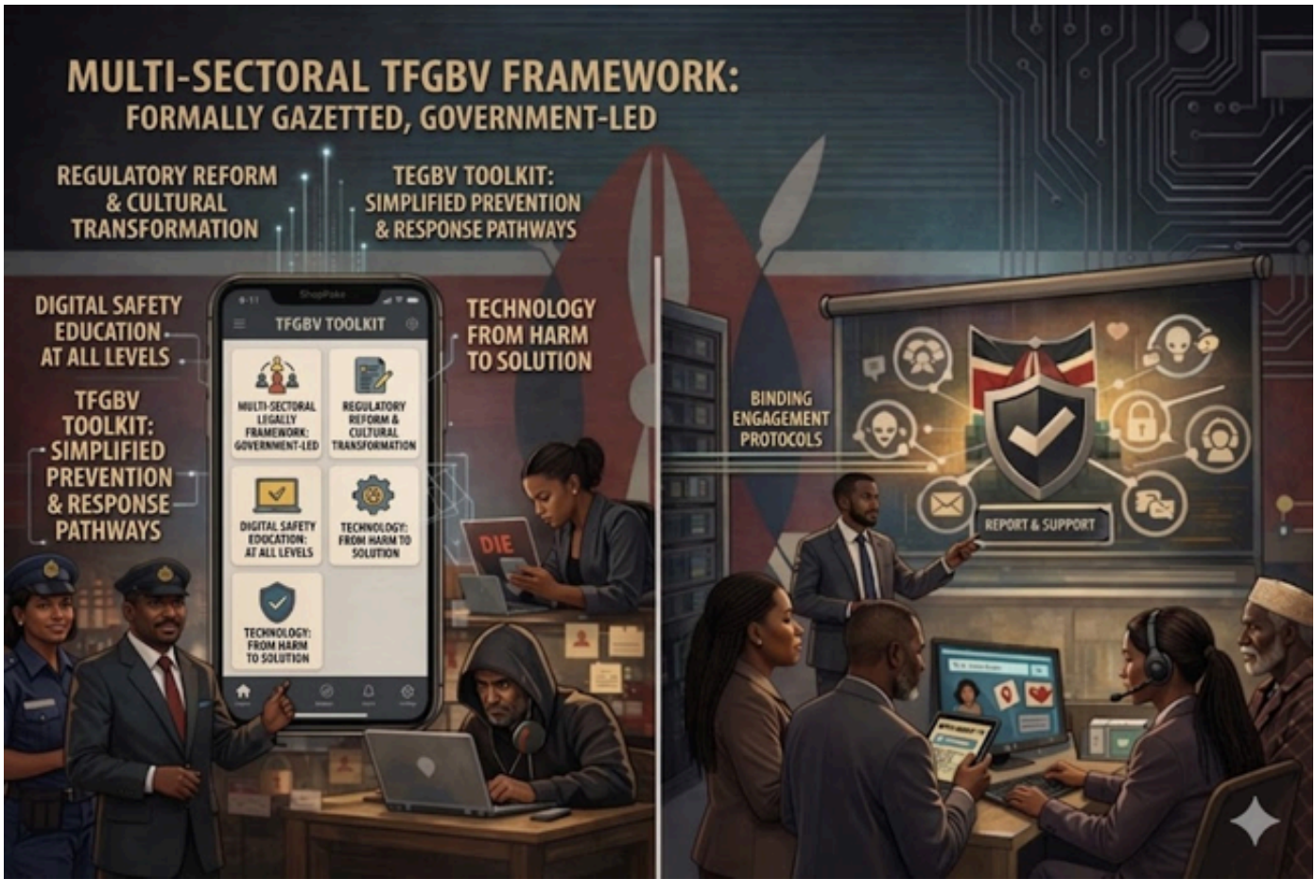
Additionally, the Ministry of Interior has required platforms to establish local presence in Kenya to facilitate takedown and coordination, with META having complied and TikTok, X, and Telegram in the process of doing so.

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. Moreover, 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 consultation generated a convergent set of recommendations that collectively inform the reform agenda presented in Chapter 7 of this report. The following principal priorities emerged with the highest level of cross-sectoral agreement i.e.:

- Creation of a formally gazetted, multi-sectoral national TFGBV coordination framework, led by government, but operational across all sectors, to replace the current fragmented ad hoc arrangements.
- Combining regulatory reform with cultural transformation, and digital safety education across all levels of the education, and the community engagement system.
- 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 to the most vulnerable populations.
- 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.
- 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.
- Structured and binding engagement with technology platforms to secure commitments on content accountability, takedown timelines, and transparency in reporting mechanisms..



CHAPTER 4.
KEY INFORMANT QUESTIONNAIRE ANALYSIS.

Key Informant Questionnaires were administered in three streams i.e., 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. The first two streams were distributed in February 2026, with responses received through March 2026.
In accordance with Kenya's Data Protection Act, 2019, all questionnaire responses are treated as confidential. Institutional roles are cited where relevant for contextual accuracy, but no individual respondent is identified by name.
This chapter synthesizes the substantive content of all three streams, identifies convergences and divergences, and draws out their collective implications for the gap analysis and reform recommendations.

4.1 STATE ACTORS AND CONSTITUTIONAL OFFICE HOLDERS.

Four substantive responses were received from state actor respondents representing institutions including the Office of the Director of Public Prosecutions, the National Police Service, the National Gender and Equality Commission, and county-level gender departments.

4.1.1 Definition and Institutional Approach to TFGBV:

Responses revealed significant variation in how state institutions define and approach 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.
This variation confirms the foundational finding from the stakeholder consultation that there is no unified, operational definition of TFGBV within Kenya's state architecture. The cascading consequences of this definitional vacuum are reflected across every subsequent theme in the questionnaire responses.
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.

4.1.2 Legal Framework Reliance:

All respondents cited the Computer Misuse and Cybercrimes Act as the primary legal instrument relied upon.
Additional frameworks cited included the Data Protection Act, the Sexual Offences Act, the Children's Act, the Counter-Trafficking in Persons Act, CEDAW, the Maputo Protocol, and the Evidence Act.
One respondent, drawing on their institution's framework, provided the most comprehensive mapping, citing domestic legislation alongside international and regional instruments including the Convention on the Rights of Persons with Disabilities and the ODPP Decision to Charge Guidelines.
The diversity of instruments cited across respondents, without any single integrated framework, reflects and confirms the patchwork legal architecture analysed in Chapter 2 of this report.

4.1.3 Adequacy of Existing Laws:

Responses to the question of whether existing laws are sufficient to address emerging forms of online harm were notably divided, reflecting a genuine institutional disagreement about the current state of the law.
One respondent argued that the CMCA applies to any existing offence committed through the use of technology, treating technology as an aggravating factor within existing criminal law, 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.
Another respondent acknowledged that Kenya had not fully tested the extent of its laws against these crimes, and called for more to be done to regulate platforms and hold them accountable.

INSTITUTIONAL DISAGREEMENT AS A GOVERNANCE FINDING.

The absence of consensus among state actor respondents on the adequacy of the current legal framework is itself a critical governance finding.
This is because 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.

4.1.4 Operational Challenges:

Operational challenges identified by state actor respondents included:

- low reporting rates among survivors 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 among investigators; and
- A general knowledge gap at all levels of the justice system.

One respondent specifically identified the challenge of inadequately trained prosecutors as the most significant operational constraint, a finding that is consistent across all three questionnaire streams.

4.1.5 Evidentiary and Jurisdictional Barriers:

All respondents acknowledged evidentiary and jurisdictional barriers. Key challenges identified included attribution difficulties arising from perpetrators' use of anonymity and encrypted platforms; the transborder nature of offences where social media platforms are foreign companies subject to different legal regimes; the difficulty of meeting the prima facie evidence threshold for TFGBV cases where digital evidence must be collected and preserved to strict legal standards; and the challenge of obtaining call data records from multinational social media operators without formal mutual legal assistance processes.
One respondent noted that coordination between the DCI, internet service providers, the Witness Protection Agency, the Attorney General, and the judiciary is currently achieved through informal cooperation, rather than through a statutory framework that mandates, structures, and monitors it.

4.1.6 Capacity Gaps:

Capacity gaps identified by state actors span technical skills, forensic tools, legal clarity, and funding simultaneously. Specific deficits noted included the absence of chain analysis investigation capacity for cryptocurrency-funded TFGBV; insufficient digital forensic tools within the DCI laboratory; lack of training for prosecutors and investigators in handling TFGBV specifically and digital evidence generally; inadequate computers and skilled officers at police stations; and chronic underfunding of specialized TFGBV units.
One respondent summarized the collective position simply as all mentioned capacity gaps exist simultaneously.

4.1.7 Recommendations from State Actor Respondents:
State actor respondents proposed the following reforms:

- A comprehensive statutory definition of TFGBV;
- Development of Standard Operating Procedures integrating TFGBV into case management across all relevant institutions;
- Creation of template charge sheets and a Rapid Reference Guide for investigators and prosecutors;
- Equipping the DCI laboratory with necessary digital forensic tools;
- Regular and mandatory training for prosecutors and investigators on emerging forms of digital harm;
- Regular community sensitization and public awareness campaigns; and
- Training on cryptocurrency investigation to address the use of virtual assets in financing TFGBV.

4.2 CIVIL SOCIETY ORGANIZATIONS AND FEMINIST GROUPS.

Nine substantive responses were received from civil society respondents representing 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.

The responses reflect a broader spectrum of GBV experience that extends beyond digital-specific TFGBV to encompass the physical, sexual, economic, and psychosocial dimensions of gender-based violence as experienced at the community level.

4.2.1 Forms of TFGBV Most Commonly Reported:

Respondents identified a range of forms reflecting both digital and broader GBV experiences across their operational contexts. Online harassment, cyberbullying, non-consensual sharing of intimate images, body shaming on social media, and persistent unwanted sexual advances through digital platforms 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, including rape, defilement, and intimate partner violence, as the most prevalent forms of GBV encountered, 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, to ensure that policy responses address the full spectrum of harm, rather than only the most visible urban digital manifestations.

4.2.2 Vulnerability Profiles:

Respondents identified multiple overlapping vulnerability profiles. 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.

Women in violent intimate partner relationships were identified as a high-risk population, particularly where partners use digital control and surveillance as instruments of ongoing coercive control.

4.2.3 Barriers to Justice:

The barriers to justice identified were consistent and convergent across all regions and operational contexts, reflecting a systemic rather than incidental pattern of exclusion from justice.

Financial barriers, including the cost of legal fees, medical reports required as evidence, and court processes, were identified as primary obstacles by the majority of respondents.

Stigma and shame were identified as major deterrents to reporting.

Lack of awareness of legal rights and available mechanisms was consistently noted, particularly in rural and informal settlement contexts.

Corruption within law enforcement and judicial processes was cited by multiple respondents as creating institutional distrust.

Cultural and community norms that normalize violence or pressure survivors into informal settlement processes, including clan negotiations that prioritize community harmony over survivor justice, were documented as significant structural barriers across multiple counties.

4.2.4 Effectiveness of Reporting Mechanisms:

Respondents were largely critical of existing reporting mechanisms. Community-based systems were identified as the most trusted and accessible mechanisms for many survivors, precisely because they operate outside the formal institutions that survivor's distrust.

Hotlines were described as effective for those with both phone access and awareness of their existence, but as systematically excluding the most vulnerable populations who cannot afford a phone or who are unaware of the services.

Law enforcement and formal justice mechanisms were characterized as inadequate due to insufficient funding, inconsistent response, lack of trauma-informed handling, and pervasive institutional distrust.

Platform-based complaint mechanisms received mixed assessments, with some respondents noted content removal within three working days, while others noted significant delays and absence of feedback. Several respondents recommended a maximum response time of one working day for the most severe TFGBV content.

4.2.5 Survivor-Centred Adequacy of Existing Laws:

No respondent characterized existing laws as fully survivor-centred in practice.

Common observations included that survivors often do not know what to do after experiencing TFGBV; that survivors face insensitive and sometimes hostile handling by authorities; that delays in investigation and limited protection during legal processes effectively punish survivors for seeking justice; and that once perpetrators complete any sentence and are released, survivors are frequently left without ongoing protection or community support, sometimes facing continued harassment or retaliation.

One respondent observed that the burden reverts entirely to the community once the justice process concludes, with no systemic provision for survivor reintegration or long-term safety planning.

4.2.6 Recommendations from Civil Society Respondents:

Respondents proposed a range of reforms and interventions, including:

- The elimination of legal fees as a barrier to access to justice in TFGBV cases;
- The development of centralized digital case recording systems to enable consistent follow-up;
- The construction of common directories of GBV actors from sub-county to national level;
- Strengthening of GBV technical working groups at county level, which respondents confirmed are effective where they are active and resourced;
- Strengthening of gender desks at police stations with TFGBV-specific training and tools;
- Expansion of mobile courts that have proven effective in bringing justice to remote communities;
- Civic empowerment programmes at the community level; and
- The construction of safe houses within every sub-county as critical infrastructure for survivors requiring emergency protection.

4.3 SURVIVORS OF TFGBV: DIRECT EXPERIENCE QUESTIONNAIRE ANALYSIS.

A third questionnaire stream was administered directly to individuals who had personally experienced TFGBV, conducted in March 2026 at the Wangu Kanja Foundation office, an organization providing support to survivors of gender-based violence.

Ten respondents participated, representing various demographics including the urban middle class, urban lower-income neighborhoods, and rural communities. They provided written responses to eleven questions exploring their experiences of online harm, their interactions with reporting and justice systems, and their 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.

All responses were collected on a confidential and anonymous basis in accordance with Kenya's Data Protection Act, 2019 and the WHO ethical guidelines for researching violence against women.

4.3.1 Respondent Demographics:

Ten respondents participated in the survivor questionnaire. The age demographics, as self-reported by respondents, were as follows: five respondents, representing 50% of the sample, were aged between 26 and 35 years; three respondents, representing 30% of the sample, were aged between 36 and 45 years; and two respondents, representing 20% of the sample, were aged between 46 and 55 years.

No respondents were recorded in the 18 to 25, 56 to 60, or over 60 age brackets.

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.

Age bracket	No 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%

4.3.2 Sense of Safety on Digital Platforms Before the Experience:

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.

This finding is significant because a clear majority of survivors approached digital platforms without a prior sense of threat or risk, indicating that TFGBV frequently strikes individuals who are not operating in a defensive posture, and who have no established framework for recognizing escalating harm.

The implication for prevention programming is 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.

4.3.3 Impact on Sense of Safety, Participation, and Wellbeing:

All nine respondents who answered this question (100%) confirmed that the online harm experienced had affected their sense of safety, participation, or wellbeing. The qualitative elaborations provided give depth and texture to this unanimous response.

One respondent permanently withdrew from a major social media platform following the experience.

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 the survivors' own testimony, the phenomenon of radio silencing documented throughout this analysis, because 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.

4.3.4 Awareness of Reporting and Support Options:

Respondents were asked whether they were aware of where to report or seek help at the time of the incident. Of the nine who answered, only two (22%) indicated that they were aware of available reporting pathways. Seven respondents (78%) indicated that they were not.

This finding is among the most consequential in the entire survey.

When more than three quarters of TFGBV survivors do not know where to turn at the time of the incident, the justice system's capacity to respond is fundamentally compromised before the reporting process even begins.
One respondent indicated that she had reported to a police station. The public awareness deficit identified by practitioners during the stakeholder consultation and confirmed by CSO respondents is here substantiated, in the direct testimony of survivors themselves.

4.3.5 Experience of Reporting:

Respondents who had reported their experience were asked whether they felt heard and supported. Of the substantive responses received, approximately 67% indicated that they did not feel heard or supported.
Specific negative experiences included:

- constant victim shaming;
- A reporting experience at a police station that the respondent characterized as being brushed off;
- Active distortion by police of information shared by the survivor; and
- Institutional revictimization at police gender desks due to instances of both male and female officers mocking complainants and making inappropriate, sexualized comments regarding intimate evidence, creating a hostile environment that further traumatizes victims and deters them from seeking justice.

Two respondents indicated that reporting was not applicable to their situation.
One respondent reported feeling supported through civil society engagement, but noted that most government entities do not follow up on cases, as compared to civil society organizations.
One respondent described a positive initial police response.

SECONDARY VICTIMIZATION AS A STRUCTURAL FINDING.

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 not anecdotal failures. They are the predictable outcomes of a system that has not made trauma-informed, survivor-centred first response a mandatory, monitored, and enforced standard across all stations and all officers.

4.3.6 Challenges Encountered in Stopping or Responding to the Harm:

Respondents described a range of challenges. Institutional barriers dominated, including enforcement officers pushing for cases to be dropped, harassment and mockery at police stations, distortion of information shared by survivors against their own interests, and gender desks that were actively hostile rather than supportive.
Personal and psychological barriers were also widely documented, including discrimination, inferiority complex, stigma, criticism, trauma, shame, and fear.
One respondent did not report at all.
Another described a general lack of information on digital security as the primary obstacle.
One respondent described a positive interaction in which she received assistance from police, underscoring that the quality of institutional response is inconsistent and dependent on individual officer conduct rather than on systemic standards.
The phrase from one respondent, there was fear especially when using social media in addition to psychological trauma from the incident, encapsulates a pattern of ongoing harm that extends far beyond the original digital violation, into the survivor's entire relationship with the digital environment.

4.3.7 Support That Would Have Been Most Helpful:

Respondents were asked what kind of support 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 the 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 and 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.
Community support was identified as important by one respondent.
The convergence of legal, emotional, and digital safety needs within individual survivors' responses reflects the holistic, interconnected nature of TFGBV harm and directly informs the recommendation developed in Chapter 7 that survivor support infrastructure must address all three dimensions concurrently, rather than treating each in isolation.

4.3.8 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.

4.3.9 Improvements Wanted from Institutions and Platforms:

Respondents' recommendations for institutional and platform improvements were substantive, specific, and convergent. They included:

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

Seven specific platforms were identified as the most problematic as regards TFGBV i.e., X (formerly Twitter), WhatsApp, the Facebook comments section, Instagram, TikTok, Telegram, and Snapchat.
One respondent described the consequences of TFGBV in terms that no policy framing can fully capture, noting that lives and livelihoods are permanently damaged post-TFGBV and that 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. This testimony places in human terms what the regulatory analysis describes in legal ones.

4.3.10 What Justice and Accountability Look Like:

Respondents' descriptions of justice and accountability reveal both a minimal threshold that is not currently being met and a clear articulation of what survivor-centred accountability would require.
Justice was described as:

- Perpetrators being held accountable;
- Survivors being supported and protected;
- Harmful content being deleted and removed from circulation;
- Cases being brought to transparent closure with all stakeholders visible through the process; 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.
One respondent offered a note of qualified hope i.e., 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.

4.3.11 What Policymakers Need to Understand:

Respondents' messages to policymakers constitute a direct brief from survivors to legislators and institutional decision-makers.

Key messages included:

- Extensive reforms are needed because implementation of existing policies is not in order and adequate resource allocation by government is essential;
- laws must be more stringent to hold perpetrators accountable and protect survivors;
- the government should enhance cybercrime laws through peer-to-peer awareness and capacity building of citizens;
- Digital harassment should be treated with the same seriousness as physical sexual gender-based violence;
- Handling of TFGBV cases should be domesticated at the ward level so that survivors do not have to travel far to access help;
- Policy makers should understand that TFGBV is not someone's fault and survivors should be protected at all times;
- Specific trained officers should be designated to handle TFGBV cases at dedicated desks; and
- More awareness must be created on handling various scenarios of TFGBV.

The collective weight of these messages is unambiguous i.e., that survivors know what they need, they can articulate it with precision and clarity, and they are not being heard.

4.3.12 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, because 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, with the majority of survivors who engaged with formal institutions, particularly police stations, experienced victim shaming, dismissal, or active hostility. This finding 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, as every respondent modified, restricted, or withdrew from digital activity as a consequence of the harm experienced, providing 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 i.e., 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.

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 cybercrimes and GBV frameworks creates definitional uncertainty that cascades through the entire justice chain, such that 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.

State actor respondents confirmed this definitional vacuum across multiple institutions and operational contexts. The stakeholder consultation documented its real-world consequences in a magistrate's inability to determine the applicable law in an active TFGBV case in 2025.

The constitutional suspension in October 2025 of key CMCA harassment provisions, analysed in detail in Section 2.2 of this report, has widened the enforcement gap further, as confirmed by the High Court proceedings in HCCRPET/E673/2025.

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 scale of this gap is underscored by the European Parliamentary Research Service 2025 finding 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 a court-admissible format.

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

The current backlog, predominately driven by a lack of personnel and decentralized facilities, results in significant secondary victimization. As evidenced by a survivor who has not had her device returned for over a year, the prolonged seizure of mobile devices compromises a victim's ability to communicate, work, and maintain economic independence. Rapid, localized forensic processing is essential to ensure that devices are imaged and released back to their owners expeditiously, preventing the 'cost of reporting' from compounding a survivor's trauma.

Furthermore, this systemic gap is exacerbated 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.

At the prosecutorial level, there is insufficient specialist capacity to handle TFGBV cases effectively. The result is a high attrition rate in TFGBV cases within the criminal justice system, with survivors disengaging at multiple points due to secondary victimization, procedural barriers, and institutional indifference. The survivor questionnaire documented this attrition in personal terms as their cases that have not moved for years, or survivors are left without information about the status of their own matters, and a pervasive sense that the legal system does not regard TFGBV as requiring urgency.

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 DCI, the ODPC, Policare, the ODPP, and the Judiciary, without any integrated referral pathway, case management system, or single point of contact.

This fragmentation creates regulatory voids, where survivors are bounced between institutions, each treating the matter as falling primarily within another's jurisdiction. The survivor questionnaire confirmed this experience directly, as respondents described cases that have not been followed up, institutions that do not communicate with each other, and survivors left to navigate parallel systems without legal support.

There is no gazetted, multi-sectoral national TFGBV coordination framework, despite widespread and consistent recognition of its necessity across all consultation streams.

Additionally, County Gender Departments, which are closest to affected communities, 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.

The absence of a survivor-centred recovery mechanism means that 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 described by the UNODC's 2025 Global Strategy on TFGBV as digital shackling.

The survivor questionnaire provided unambiguous evidence of this gap, because respondents described lives and livelihoods permanently damaged, entire relocations undertaken for personal safety, and the need to restart life again with nothing, because harmful content destroying community relationships could not be removed from online circulation.

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 the production of synthetic intimate audio, nudify application outputs, and AI-generated disinformation campaigns targeting women are all entirely outside the scope of current legislation.

Kenya's National AI Strategy 2025 to 2030 does not address the gendered dimensions of AI risk. The Artificial Intelligence Bill 2026, currently before the Senate, represents the most significant current legislative opportunity to embed gender-responsive AI governance in statute. However, it requires substantial amendment before it can serve as an effective instrument for addressing TFGBV: 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 ODPC and NC4 mandates rather than creation of three parallel regulatory bodies; mandatory adversarial robustness testing; and electoral AI disinformation provisions.

Platform monetization models, which algorithmically amplify engagement-generating TFGBV content, must also be addressed through formal platform accountability obligations.

5.6 SOCIO-CULTURAL AND AWARENESS GAPS.

A structural and pervasive barrier to TFGBV prevention and response is the low level of awareness within communities, institutions, and the general public about the nature, prevalence, and legal status of TFGBV. The survivor questionnaire confirmed this directly, as 78% of respondents who had experienced TFGBV did not know where to report or seek help at the time of the incident.

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 in ways that compound legal failures.

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. Survivors rarely receive trauma-informed care, psychosocial support, or referral to specialized services when engaging with formal justice institutions.

5.7 CHILDREN AND MINORS: A CRITICAL AND CURRENTLY UNPROTECTED POPULATION.

TFGBV against girls does not begin at adulthood, rather it begins in school, in the digital learning platforms, peer messaging groups, and social media ecosystems that form the social infrastructure of Kenyan adolescence.
Research published by the United Nations Population Fund demonstrates that 64.4% of female students in Nairobi's higher learning institutions have personally experienced online violence, nearly double the rate of their male peers.
The rollout of Kenya's Competency Based Curriculum 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. Kenyan children are being algorithmically assessed and their data harvested in classrooms where parents have no legal mechanism to object. This is not a future risk, but a current, ongoing harm with no legal remedy.
Beyond the classroom, 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 that prevention frameworks must address. Advertising AI targets children with a precision and persistence that previous generations of marketers could not achieve, exploiting psychological vulnerabilities in real time, without parental awareness or regulatory oversight.

THE CHILDREN'S AI PROTECTION GAP: CURRENT HARM, NOT FUTURE RISK.

The Artificial Intelligence Bill 2026 contains no provision specifically protecting minors from AI systems.
This is not a gap about a future risk, rather it is a gap about harms that are occurring in Kenyan schools and on Kenyan children's devices right now.
Every month that passes without this protection is another month in which children's behavioural, emotional, and learning data is harvested without consent, girls are exposed to AI-driven content that facilitates grooming and exploitation, and the algorithmic foundations of a generation's digital identity are laid without oversight, accountability, or legal remedy.

A dedicated children's AI protection provision in the AI Bill should prohibit 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 and a meaningful opt-out mechanism.
The design of these protections should be grounded in the UN Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in the Digital Environment (2021) as the authoritative international standard, and should be consistent with Kenya's constitutional obligations under Article 53.

5.8 DEMOGRAPHIC DISAGGREGATION: INTERSECTING VULNERABILITIES.

A feminist and rights-based gap analysis must disaggregate vulnerability profiles, rather than treating all women and girls as a homogeneous population. Four population groups whose experiences of TFGBV are shaped by intersecting forms of marginalization, require specifically tailored legal and institutional responses, that the current framework does not provide.

5.8.1 Women with Disabilities: Digital Exclusion and Heightened Vulnerability:

Women with disabilities face a dual barrier in the TFGBV context, as they are both disproportionately vulnerable to digital violence, and disproportionately excluded from the literacy, reporting mechanisms, and support systems required to address it. Further, women with cognitive or psychosocial disabilities face elevated exploitation risks.
Reporting mechanisms and survivor support services are frequently inaccessible to women with visual, hearing, or cognitive disabilities.
Kenya's constitutional obligations under Article 54 and the Convention on the Rights of Persons with Disabilities require that all survivor-facing systems comply with Web Content Accessibility Guidelines at minimum level AA as a design standard from inception rather than as a retrofit.

5.8.2 Elderly Women: Invisible Survivors in the Digital Age:

Elderly women in Kenya represent an almost entirely invisible population in the TFGBV discourse, yet they face specific and documented forms of technology-facilitated harm including social engineering and digital financial fraud, coercive control by family members over mobile money and digital financial services, and the weaponization of digital platforms to facilitate property disinheritance and economic exclusion of widows.

National TFGBV awareness and prevention programmes must reach elderly women through community radio, in-person community engagement, and faith-based networks, rather than exclusively through digital channels that may be inaccessible to them.

5.8.3 Men and Boys: Secondary Victims and Supply-Side Actors:

A comprehensive TFGBV analysis for the wellbeing of all Kenyans must acknowledge that men and boys are affected both as secondary victims, through the economic and relational harm caused when female family members are targeted, and as individuals shaped by algorithmic ecosystems that normalize misogyny. The recommended legal framework should use gender-neutral drafting for its protective provisions while incorporating gender-specific analysis of risk profiles and remedy requirements, ensuring that women receive the targeted protection they require and that male victims are not structurally excluded from legal recourse.

5.9 THE MANOSPHERE AND ALGORITHMIC AMPLIFICATION: ADDRESSING THE SUPPLY SIDE OF TFGBV.

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, documented by the Global Network on Extremism and Technology and the Centre for Countering Digital Hate, that systematically produces and distributes content dehumanizing women, normalizing coercive control in intimate relationships, and coordinating targeted harassment campaigns against individual women who publicly challenge misogynist discourse.

Its Kenyan manifestations also 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.

Furthermore, these digital harms extend beyond the youth, because the algorithmic amplification of misogyny increasingly targets Kenyan men in their twenties, thirties, and forties. This is particularly evident among those navigating relationship breakdowns or personal crises, where online echo chambers exploit their vulnerabilities to entrench hostile narratives that further undermine women’s agency and social cohesion.

The business models of major social media platforms are structurally misaligned with TFGBV prevention. Platforms monetize engagement, and their algorithmic systems demonstrably amplify content that provokes strong emotional responses, including coordinated harassment and intimate image abuse. Platforms are not passive hosts of TFGBV content. They are active amplifiers whose commercial incentive structures directly incentivize the propagation of harm. The AI Bill's risk classification framework provides the legislative vehicle through which algorithmic accountability for TFGBV amplification can be established, requiring content recommendation systems deployed by major platforms to undergo mandatory gender-disaggregated algorithmic impact assessments.

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 / 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 criminalization 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.

Demographic Group	Primary TFGBV Risk Vectors	AI-Specific Vulnerability	Key Legal / Policy Gap
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 M-Pesa 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 radicalization 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.

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.
An estimated 98% of all deepfake content constitutes non-consensual sexual imagery, and 99% of that content targets women and girls, as documented by the Security Hero State of Deepfakes Report (2023) and confirmed by the European Parliamentary Research Service (2025).
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 NCII. In the specific context of Kenya's 2027 electoral cycle, the combination of deepfake technology, with high mobile penetration, and limited digital literacy creates conditions in which AI-enabled electoral TFGBV, could materially influence political outcomes, and silence women candidates, a risk that demands both legislative criminalization and public digital literacy investment at scale.

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, if inadequately governed, 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 intersection of digital ID systems with TFGBV contexts is particularly acute, because 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, limiting law enforcement's ability to enforce takedown orders, obtain user data, and hold platforms accountable. While META has complied with the Ministry of Interior's requirement for local presence, others remain partially outside Kenya's regulatory reach.
The Google Global Transparency Report of February 2026 recorded that Kenya's government content removal requests were rejected at a rate of approximately 62% in the first half of 2025, providing quantitative evidence of the platform compliance gap that formal statutory obligations must address.
Moreover, as platforms evolve their monetization models toward increasingly algorithmic content amplification, the risk of TFGBV content being systematically promoted to maximize engagement will intensify.

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 questionnaire 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 for a future-proofed response architecture.

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, documented in Johns Hopkins Bloomberg School of Public Health research (2024) which 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 rather than adopting a one-size-fits-all approach.

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. Unlike classical computers that process bits sequentially, quantum computers utilize qubits, units capable of existing in multiple states simultaneously, enabling them to perform specific cryptographic calculations millions of times faster than the world's most powerful conventional supercomputers. While fault-tolerant quantum hardware is currently concentrated in the Global North, milestones reached in 2025 and 2026 indicate that practical, cloud-based quantum-as-a-service is moving toward commercial availability, within a timeframe that demands immediate legislative and institutional preparation, rather than deferred response.

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, including active TFGBV cases, encrypted survivor testimonies, and confidential communications between investigators and prosecutors, 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 by adversaries, rendering today's confidentiality guarantees retroactively void. Without an immediate transition to Post-Quantum Cryptography and a modernized evidence preservation framework, the confidentiality and integrity of Kenya's current and future judicial records face a retroactive and irreversible breach, with profound consequences for survivor safety, prosecutorial integrity, and judicial accountability in TFGBV cases.

The legal admissibility frameworks currently being developed for digital evidence in Kenya must therefore 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.

This is not a future upgrade consideration, rather it is a present design requirement and as such, all DCI laboratory investments recommended in this report, all evidence preservation protocols developed under the Evidence Act amendments proposed in Chapter 2, 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, thereby ensuring that Kenya's investment in digital justice infrastructure today, does not become a liability when quantum capabilities arrive.

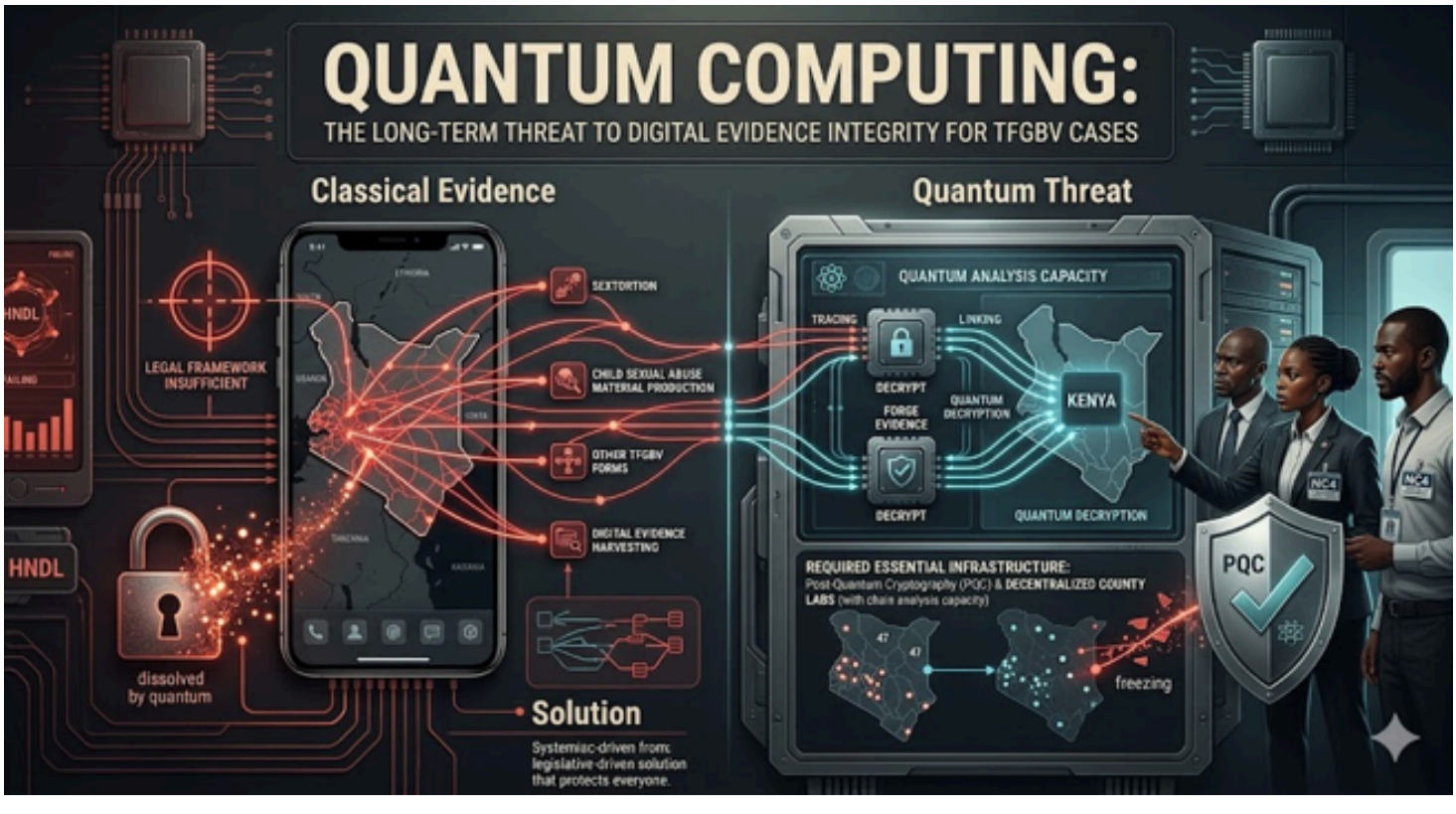
6.7 AI CYBERSECURITY THREAT VECTORS: MODEL POISONING AND PROMPT INJECTION.

The Artificial Intelligence Bill 2026 does not address AI-specific cybersecurity threat vectors, an omission that is significant for Kenya, a country ranked twenty-first on the International Telecommunication Union's Global Cybersecurity Index.

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, because 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.

The AI Bill should require mandatory adversarial robustness testing for all high-risk AI systems deployed in Kenya's justice, health, and social services contexts.



CHAPTER 7.
RECOMMENDATIONS AND WAY FORWARD.

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 NCII, 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) should inform the drafting process throughout, alongside the ACHPR Resolution 522 on the Protection of Women Against Digital Violence in Africa and the AU Convention on Ending Violence Against Women and Girls adopted in February 2025.

7.1.2 Urgently Redraft the Suspended CMCA Provisions:

The constitutional suspension of Section 27(1)(b), (c), and (2) of the Computer Misuse and Cybercrimes Act has created an enforcement vacuum that demands 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 to ensure the balance between harm prevention and expression protection is properly calibrated in statute. The redrafted provisions should also introduce:

- **explicit criminalization of AI-generated NCII;**
- **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 Data Protection Act, 2019 requires amendment to:

- **introduce aggravated harm provisions for the weaponization of personal data in TFGBV contexts;**
- **ensure emergency erasure and content removal powers exercisable by the ODPC within hours of a verified TFGBV complaint;**
- **warrant mandatory safety by design obligations on social media platforms operating in Kenya;**
- **guarantee statutory integration with criminal justice referral mechanisms; and**
- **establish provisions recognizing the heightened sensitivity of data held in intimate partner contexts where technology is used as a tool of coercive control.**
-

7.1.4 Amend the Sexual Offences Act:

The Sexual Offences Act, No. 3 of 2006 should be amended to extend its definitional framework, to virtual and technology-mediated sexual offences, explicitly including AI-generated non-consensual sexual imagery, sextortion, and digital sexual coercion, with a technology-facilitated sexual offences schedule added as an annex.

7.1.5Amend the Protection Against Domestic Violence Act:

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, encompassing digital surveillance, digital coercive control over financial accounts or communication devices, and the use of intimate images as instruments of intimidation. Courts should be required to include specific digital protection provisions within protection orders issued.

7.1.6 Amend KICA to Establish Enforceable Platform Accountability:

The Kenya Information and Communications Act, 2013 should be amended to:
v introduce a statutory Urgent Digital Protection Order mechanism, enabling expedited judicial orders with twenty-four-hour compliance timelines, enforceable against platforms irregardless of country of incorporation;
v guarantee conditional platform liability for TFGBV-enabling conduct;
v establish mandatory localized content moderation requirements for platforms with more than one million Kenyan users;
v ensure mandatory transparency and annual reporting obligations; and
v provide data localisation requirements to facilitate evidence access.

7.1.7 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.

7.2.1 Establish a National TFGBV Coordination Framework:

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.

7.2.2 Invest in Digital Forensic Capacity:

The DCI laboratory requires urgent investment in digital forensic tools and specialist capacity, with post-quantum resilience as a mandatory design requirement.
Mandatory digital forensic training for cybercrime investigators should be established with specific modules on TFGBV evidence collection, cryptocurrency tracing, and AI-generated content analysis.
NC4's Rapid Reference Guide and Template Charge Sheets should be formally gazetted and operationalized across all police stations and prosecutor offices.

7.2.3 Build Specialist Prosecution Capacity:

The ODPP should establish specialized TFGBV prosecution units with dedicated trained prosecutors.
Further, regular, mandatory training on TFGBV case law, digital evidence standards, AI-enabled harms, and trauma-informed practice should be institutionalized.
The ODPP's Decision to Charge Guidelines should be updated specifically to address TFGBV charging decisions, drawing on the framework provided by the Maputo Protocol and CEDAW General Recommendation No. 35 (2017).

7.2.4 Strengthen County-Level Response:

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

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 in Section 7.1.6, 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, to advocate for global adoption of Safety by Design standards, as a mandatory baseline for AI systems.

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 CSOs, CBOs, and community health workers;
- operationalization of the KICTANet OGBV Tracker as a national data aggregation and case monitoring tool; and
- the 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.
A national TFGBV data observatory should be supported in collaboration with research institutions and civil society.
The NGEC should be specifically empowered and resourced to publish a biennial TFGBV report.
Kenya's National AI Strategy 2025 to 2030 should be supplemented with a gender-responsive AI governance framework.
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.
Kenya should also ratify the ILO Convention 190 on Violence and Harassment (2019) 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;
- prevent 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 existing institutional framework recommended throughout this report, specifically 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 would deliver 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 and sustaining a new commission.
The evidence presented in this analysis is unambiguous that institutional fragmentation is already one of the most critical structural failures in Kenya's TFGBV response architecture.

Designating the Ministry of Education as a co-regulator working through existing institutional mandates, rather than through a new and undefined relationship with a proposed AI Commissioner whose jurisdictional boundaries remain unclear in the current Bill, is both the more cost-effective and the more survivor-centred solution. It ensures that the child protection, data governance, and harm prevention functions required in educational AI deployments are administered by bodies with established expertise, existing accountability mechanisms, and direct lines to the justice and support systems that children and their families would need to access if harm occurs.

Additionally, 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.

7.8 ADDRESSING THE ARTIFICIAL INTELLIGENCE BILL 2026: INTEGRATED RECOMMENDATIONS.

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

- The Bill should 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 replacing the current fragmented multi-agency approach.
- The risk classification framework should be amended 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, consistent with the approach taken under the EU Artificial Intelligence Act, 2024.
- The Bill should 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.
- The compliance framework for open-source model deployers should be amended 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.
- Specific electoral AI provisions should be introduced, including mandatory labelling of AI-generated political content and a prohibition on synthetic political impersonation content in the twelve months preceding a general election.
- The penalty structure should 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, as documented in the UN Women Tipping Point Report (2025) and in the research of the Association of Media Women in Kenya which 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.
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 as the evidential basis for dedicated TFGBV digital safety budget allocations, consistent with Kenya's commitments under SDG 5 and SDG 16.
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 Bill's mandate for the AI Commissioner 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 CBO networks as primary delivery channels, consistent with Kenya's commitments under AU Agenda 2063 and the AU Digital Transformation Strategy for Africa 2020 to 2030.

Furthermore, Kenya should develop and adopt a National Digital Safety and TFGBV Prevention Strategy as a distinct policy instrument, separate from but aligned with the National AI Strategy, the National Cybersecurity Strategy, and the National GBV Action Plan, with measurable targets and annual progress reporting to Parliament.
Finally, 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.

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, and that 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 & 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 what it has the capacity to be i.e., 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.

Acronym	Full Title and Contextual Note
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.
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.
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