

Assessing the adequacy of Zimbabwe's Legal and Policy Frameworks in addressing Technology-Facilitated Gender-Based Violence

Octavious Chido Masunda

National University of Science and Technology, Zimbabwe

DOI: <https://doi.org/10.51244/IJRSI.2026.1315PH00181>

Received: 16 September 2026; Accepted: 21 September 2026; Published: 01 October 2026

ABSTRACT

This paper assesses the adequacy of Zimbabwe's legal and policy frameworks in addressing TFGBV and identifies gaps, challenges and prospects for reform. Anchored in feminist legal theory, cyberfeminism and intersectionality, the study combines a documentary analysis of nine legal and policy instruments, including the recently adopted National Artificial Intelligence Strategy (2026-2030) and the National Child Online Protection Policy (2026-2030), with thirteen semi-structured interviews across government, law enforcement, civil society, the ICT sector and intergovernmental organisations. Each instrument is assessed against four criteria covering recognition of gendered harm, coverage of digital offences, enforcement and survivor support, and cross-sectoral coordination. Findings show that the framework remains fragmented and gender-blind, and that its enforcement is selective rather than simply weak. The cyber provisions punish harm to reputation up to twice as heavily as the non-consensual recording of a person's body, and the reported prosecutions concentrate on the former. The two newest instruments repeat the pattern. The AI Strategy names deepfakes as a threat to the state and to public trust but is silent on their use as instruments of sexual abuse against women, while the Child Online Protection Policy adopts a protectionist orientation whose safeguards end at the age of majority. The paper proposes a multi-sectoral framework linking ICT policy, the national gender machinery and survivor-centred support and identifies the revision of the Cyber and Data Protection Act mandated by the AI Strategy as the immediate entry point for gender-responsive digital governance.

Keywords: Technology-facilitated gender-based violence, feminist legal theory, cyber governance, artificial intelligence policy, digital rights, intersectionality, Zimbabwe

INTRODUCTION

Digital technologies have reshaped how societies communicate, trade and participate in public life, and the same transformation has opened new channels for gender-based violence (GBV). Technology-facilitated gender-based violence (TFGBV) covers a range of digital harms, including cyberstalking, non-consensual sharing of intimate images, online harassment and coordinated abuse, that disproportionately affect women and girls (Henry and Powell, 2018, UN Women, 2022). Digital devices and platforms have become instruments through which existing patterns of patriarchal control are extended into online spaces (Powell and Henry, 2017).

Zimbabwe presents a compelling setting for examining this problem. Internet penetration has expanded rapidly while gender inequality remains entrenched, and recent evidence indicates that women journalists, politicians and activists face sustained online abuse designed to silence them (Mtero et al., 2023, Zirima and Sithole, 2025). At the same time the country has been building a digital governance architecture at speed. The Cyber and Data Protection Act was enacted in 2021, a revised National Gender Policy was adopted in 2025 and in 2026 the Government launched the National Artificial Intelligence Strategy (2026-2030) and approved the National Child Online Protection Policy (2026-2030). Whether this expanding architecture recognises and redresses the gendered character of online harm is the question this paper pursues.

The study addresses three research questions. First, to what extent do Zimbabwe's legal and policy frameworks recognise and address TFGBV? Second, how do institutional practices and socio-cultural norms shape enforcement and survivors' access to justice? Third, what prospects exist for embedding gender justice in the

country's evolving digital governance architecture, including the new AI Strategy and Child Online Protection Policy?

LITERATURE REVIEW

Conceptualising TFGBV

TFGBV refers to abuse, harassment and intimidation perpetrated through digital technologies. Scholars define it as a spectrum of behaviours, including cyberstalking, online harassment, doxxing, image-based sexual abuse and the non-consensual sharing of intimate content, that replicate and intensify offline gender inequalities (Henry and Powell, 2018, Jane, 2017). UN Women (2022) treats it as part of a continuum of GBV that restricts women's participation, safety and expression online. Its spacelessness allows perpetrators to transcend geographical boundaries (Harris and Woodlock, 2019) and its harms merge psychological, reputational and sexual injury with data misuse, a combination that legal systems designed for physical harm struggle to capture. A survey across thirty-one countries found that 58 percent of girls and young women had experienced online harassment (Plan International, 2020), with women, children and marginalised groups bearing the heaviest burden (Bansal et al., 2022, Esposito and Semenzin, 2025).

Global perspectives and legal responses

Feminist digital scholars argue that online violence is not a novel phenomenon but a technological extension of patriarchal control over women's voices and bodies (Citron, 2014, Dragiewicz et al., 2018), although these debates emerge from contexts with comparatively strong digital governance. Whether TFGBV is best treated as cybercrime or as a form of GBV remains contested, the first framing centring technology misuse and individual perpetrators and the second patriarchal social relations (Powell and Henry, 2017). Individualistic approaches have been criticised for ignoring structural oppression and for producing criminal justice responses that fall hardest on marginalised communities (Bailey, Flynn and Henry, 2021). Dunn (2021) demonstrates that harmful technology-facilitated behaviours constitute violence under established frameworks, while Yardley (2021) reads such abuse as a manifestation of patriarchal power within contemporary political economy. Legal responses in these jurisdictions have largely expanded existing harassment and stalking law to cover digital communication, an approach feminist critics read as reactive, punitive and inattentive to prevention and survivor-centred justice (Suzor et al., 2018).

African policy responses

Across Africa rising internet access has been accompanied by intensifying online violence against women while regional frameworks are still maturing. More than thirty-five African countries have enacted data protection laws over the past decade (Greenleaf and Cottier, 2021, Makulilo, 2015). The Malabo Convention of 2014 establishes privacy principles and mandates independent data protection authorities, although ratification remains incomplete (Orji, 2018, Bande, 2023), the African Declaration on Internet Rights and Freedoms opposes mass surveillance (Abdulrauf and Fombad, 2016, Sutherland, 2018), the ECOWAS Personal Data Protection Act binds West Africa (Abdulquadir, 2020) and SADC has adopted a model law (Boshe et al., 2022). Most directly relevant here, Resolution 522 adopted by the African Commission on Human and Peoples' Rights in 2022 addresses the protection of women against digital violence (ACHPR, 2022).

Country evidence shows a recurring pattern in which cybercrime and data protection laws exist but rarely recognise the gendered dynamics of online violence. South Africa's Films and Publications Amendment Act of 2019 criminalises distribution of intimate images without consent yet enforcement remains weak.

Gender-based violence and digital governance in Zimbabwe

GBV remains widespread in Zimbabwe. A review of a decade of empirical research indicates that close to half of Zimbabwean women report experiencing some form of physical, sexual or emotional violence in their lifetime (Bengesai and Chikhungu, 2025). Research on the digital dimension is newer but pointed. A study of women journalists found that 63 percent had experienced TFGBV (Zirima and Sithole, 2025) and analyses of

online political discourse show that gendered abuse contributes to the silencing and withdrawal of women in public life (Mtero et al., 2023). Digital inequality intersects with these harms since women's access to and use of ICTs remains uneven across class and geography (Zindi et al., 2025). Zimbabwe's response is spread across the 2013 Constitution, the Domestic Violence Act [Chapter 5:16], the Criminal Law (Codification and Reform) Act [Chapter 9:23], the Cyber and Data Protection Act [Chapter 12:07], the National Gender Policy (Ministry of Women Affairs, Gender and Community Development, 2025), the National ICT Policy (Government of Zimbabwe, 2022) and now the National Artificial Intelligence Strategy (Government of Zimbabwe, 2026a) and the National Child Online Protection Policy (Government of Zimbabwe, 2026b). These instruments constitute the documentary corpus analysed below.

Theoretical framework

TFGBV sits at the intersection of law, technology and social power. The study draws on three interrelated perspectives.

Feminist legal theory (FLT) examines how laws reflect and reproduce gendered power, challenging the assumption of legal neutrality by exposing how patriarchal norms shape legal definitions, priorities and enforcement. Applied to TFGBV, it reveals how cybercrime and data protection laws may trivialise gendered online abuse by treating it as a general offence rather than a violation rooted in unequal gender relations.

Cyberfeminism complements FLT by focusing on gender and technology. Digital spaces can both empower and endanger women, and technological systems reflect the values of their creators. In Zimbabwe, where rapid digitalisation coexists with entrenched gender inequality, cyberfeminism illuminates technology as a site of both emancipation and control and exposes the inadequacy of frameworks that fail to integrate agency, consent and bodily autonomy into online safety policy (Mhajne and Whetstone, 2024).

Intersectionality, developed by Crenshaw (1989), recognises that experiences of TFGBV are shaped by overlapping structures of class, geography, age, disability and digital access. Rural women, young women and those with limited digital literacy command fewer avenues for redress. Laws requiring formal reporting or digital evidence exclude victims without connectivity or technical skill, while urban-based enforcement leaves remote communities unprotected. Intersectionality thus broadens the analysis to structural vulnerability, including what Crenshaw termed intersectional invisibility (Coles and Pasek, 2020).

METHODOLOGY

Research design

The study adopted a qualitative design combining documentary analysis with semi-structured interviews, suiting a question that concerns both the content of legal texts and the institutional practices through which they are applied. The three theoretical lenses guided interpretation throughout.

Nine instruments were analysed. These were the Constitution of Zimbabwe (2013), the Domestic Violence Act [Chapter 5:16], the Criminal Law (Codification and Reform) Act [Chapter 9:23], the Cyber and Data Protection Act [Chapter 12:07], the National Gender Policy (2025), the National ICT Policy (2022-2027), the POTRAZ Child Online Protection Guidelines (2015), the National Artificial Intelligence Strategy (2026-2030) and the National Child Online Protection Policy (2026-2030). Each was assessed against four criteria, namely whether it recognises TFGBV as a gendered harm, whether it covers specific digital offences including emerging AI-enabled abuse, whether it provides enforcement procedures and survivor-centred support, and whether it assigns coordination responsibilities across the gender and ICT sectors. The assessment is summarised in Table 2.

One limitation of the corpus should be stated at the outset. The full text of the Child Online Protection Policy had not been publicly released at the time of writing. The assessment of that instrument therefore draws on the official post-Cabinet summary of its objectives and nine strategic focus areas and on ministerial statements about its orientation. That reading is preliminary rather than doctrinal and is presented as such throughout, and a full textual analysis should follow release of the policy document.

Semi-structured interviews

Thirteen key informants were purposively selected for their institutional knowledge of gender, law and digital governance in Zimbabwe. Selection targeted the ministries, statutory bodies and organisations with direct mandates over TFGBV, and the sample size reflects the small population of actors holding such mandates. Table 1 summarises the participants, who are identified by code to protect anonymity.

Table 1. Interview participants

Code	Sector	Role type
P1	Government (justice)	Legal officer
P2	Government (ICT)	Policy official
P3	Government (women's affairs)	Policy official
P4	Law enforcement	Victim Friendly Unit officer
P5	Law enforcement	Officer, cybercrime portfolio
P6	Civil society	GBV survivor support organisation
P7	Civil society	GBV survivor support organisation
P8	Civil society	Women's rights coalition
P9	Civil society	Women's rights coalition
P10	Legal practice	Women lawyers association
P11	Legal practice	Women lawyers association
P12	ICT sector	Data analyst
P13	International agency	Gender specialist

Data analysis

Transcripts and documents were analysed thematically following Braun and Clarke (2006), combining deductive categories from the theoretical framework with inductive codes emerging from the data. The study received clearance from the NUST Institutional Review Board, reference NUST/IRB/2026/114, prior to data collection. Participants gave informed consent and confidentiality was protected through the coding system reported above.

FINDINGS

The documentary analysis assesses the nine instruments against the four criteria. The interview findings are then organised under six themes, followed by an account of the points on which respondents diverged.

Documentary analysis of the legal and policy framework

The Constitution of Zimbabwe

The 2013 Constitution provides a strong foundation. Sections 51 to 56 guarantee dignity, equality, personal security and freedom from all forms of violence whether public or private, section 80 obliges the state to prevent domestic violence and the Gender and Human Rights Commissions may investigate violations. Section 57 protects privacy, but the text makes no reference to digital rights, data protection or online safety, and its silence on artificial intelligence and cyber harassment leaves interpretation dependent on subordinate legislation.

The Domestic Violence Act

The Domestic Violence Act [Chapter 5:16] of 2006 recognises physical, emotional, sexual and economic abuse, establishes protection orders and coordinates police, courts and social welfare officers. Its coverage of harassment, intimidation and stalking could in principle extend to some online conduct, but the Act predates the digital era. It does not name online harassment, cyberstalking, image-based sexual abuse or synthetic media abuse and contains no provisions for digital evidence, online reporting or cooperation with service providers. Protection orders do not reach online environments.

The Cyber and Data Protection Act

The Cyber and Data Protection Act marks a significant advance, but its architecture is often misread. It does not operate as a freestanding criminal statute. It amended sections 162 to 166 of the Criminal Law (Codification and Reform) Act and inserted a cybercrime part into it,¹ so the offences it creates are charged and tried as Code offences. Alongside this it establishes cybersecurity and data protection institutions and designates POTRAZ as the Data Protection Authority.

Four inserted provisions bear directly on TFGBV. The first criminalises the recording of genitalia and buttocks and the up-skirting or recording of nude images without consent.² The second criminalises cyber-bullying and harassment, reaching any data message generated, sent or posted with intent to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress, or to degrade, humiliate or demean another person, or to encourage self-harm.³ The third criminalises the transmission of false data messages about an identifiable person with intent to cause psychological or economic harm.⁴ The fourth criminalises the transmission of intimate images without consent.⁵

Assessed against the study's criteria, the substance of these provisions is more revealing than their presence. None names gender. Harm is defined by the medium and the accused's state of mind rather than by the structural relation between perpetrator and victim, so a statute that could have recognised TFGBV as gendered violence instead constructs it as misuse of an information system. The penalty structure carries the point further. Cyber-bullying, which protects against humiliation and emotional distress, attracts up to ten years. Non-consensual recording of a person's body attracts five. Within a single statute enacted on a single day, the provision safeguarding reputation is punished twice as heavily as the provision safeguarding sexual autonomy. The Act also provides no survivor-centred reporting route, no expedited takedown, no duty of cooperation on platforms and no allocation of responsibility between the Data Protection Authority, the Gender Commission and the police.

The Criminal Law (Codification and Reform) Act

Because the cyber offences sit inside the Code, that statute is now both Zimbabwe's general penal framework and the vehicle for digital harm. Three seams open where the two meet. The first is definitional. The Code's sexual offences turn on physical contact or physical presence while the inserted provisions turn on transmission, and conduct that is sexual in character but digital in execution can fall between them. The second is relational. Nothing connects the cyber offences to the concept of a domestic relationship in the Domestic Violence Act, so a partner or former partner who circulates intimate images is charged as a cyber offender rather than as a perpetrator of domestic violence, and the pattern of coercive control does not appear on the charge sheet. The third is technological. The intimate images provision turns on an image of the complainant, which leaves synthetic imagery that is not a recording of her arguably outside its reach, while the false data messages provision requires both falsity and intent to cause psychological or economic harm, an awkward fit for sexual imagery whose harm is not that it is believed. Deepfake sexual abuse therefore has no secure home

¹Cyber and Data Protection Act [Chapter 12:07] (2021), long title.

²Criminal Law (Codification and Reform) Act [Chapter 9:23] sec 164A (as inserted by the Cyber and Data Protection Act (n 1)).
Penalty: level 10 fine or imprisonment not exceeding five years.

³Criminal Law Code (n 2) sec 164B. Penalty: level 10 fine or imprisonment not exceeding ten years.

⁴Criminal Law Code (n 2) sec 164C. Penalty: level 10 fine or imprisonment not exceeding five years.

⁵Criminal Law Code (n 2) sec 164E.

in the Code. Investigative procedure also remains traditional, with no mandate for digital forensic capacity or survivor protection during investigation.

A fourth feature is the breadth of the cyber-bullying provision. Its reference to degrading, humiliating or demeaning another person is capacious enough to capture reputational insult, which makes it available to any complainant with the standing to invoke it.

Reported prosecutions offer a preliminary indication of how this operates. In March 2026 a Harare woman was charged and convicted of cyber-bullying for a TikTok video insulting a businesswoman.⁶ In the same year a social media personality faced cyber-bullying charges in which a police cyber expert testified to forensic examination linking her to Facebook and WhatsApp posts, a matter that had not concluded when this paper was written.⁷ No reported prosecutions for non-consensual recording or for transmission of intimate images were identified in the sources reviewed. That observation rests on media reporting rather than court records, and absence may reflect underreporting rather than non-enforcement. It is nonetheless consistent with the penalty structure. The provisions being used are those that protect reputation.

The National Gender Policy

The National Gender Policy (2025) recognises women's access to digital technologies and commits to a survivor-centred response to GBV, cross-sectoral collaboration and capacity building. Yet it contains no definition or recognition of TFGBV. Cyberstalking, non-consensual image sharing and online sexual harassment are unnamed, there are no operational guidelines for digital evidence and the monitoring framework carries no TFGBV indicators, so the gendered dimension of online harm remains statistically invisible.

The National ICT Policy

The National ICT Policy (2022-2027) acknowledges gender equality in ICT access, promotes safe digital practices and provides for cybersecurity structures including a national computer incident response team. It nonetheless does not recognise TFGBV as a form of harm, and its cybersecurity provisions centre on infrastructure rather than individual safety, digital evidence handling or survivor redress.

The POTRAZ Child Online Protection Guidelines

The Child Online Protection Guidelines issued by POTRAZ in 2015 were Zimbabwe's earliest instrument on online safety, giving age-graded advice to children on grooming, cyberbullying, privacy and reporting channels including Childline and police Victim Friendly Units (POTRAZ, 2015). They are educational rather than regulatory and are framed in gender-neutral terms even though the harms they describe fall disproportionately on girls.

The National Artificial Intelligence Strategy 2026-2030

Cabinet approved the National Artificial Intelligence Strategy in October 2025 and the President launched it in March 2026. It is organised around six pillars covering talent, infrastructure, adoption, governance, research and international collaboration, and grounds AI governance in an Ubuntu-based ethic of collective responsibility and human dignity (Government of Zimbabwe, 2026a). Assessed against the study's criteria it registers gender in distributional terms. Inclusive development provisions require gender equality measures in development teams and gender impact assessments, women's groups are named among participants in proposed community AI councils and women-led enterprises are targeted for MSME support. The risk

⁶S v Phiri (Harare Magistrates Court, March 2026), reported as 'Harare woman pleads guilty to cyber-bullying businesswoman Zodwa Mkandla in TikTok video' NewZimbabwe (10 March 2026) and 'TikToker sentenced for cyberbullying businesswoman Zodwa Mkandla' (12 March 2026). The accused was charged under sec 164B in respect of a video posted on 4 March 2026. Reported sentences vary across sources and should be verified against the court record.

⁷'Cyber expert links socialite Jeke to alleged cyberbullying posts' NewsDay Zimbabwe (21 July 2026). Charges brought under the cyber-bullying provision; the State closed its case and the matter was unconcluded at the time of writing.

framework acknowledges that AI trained on biased data can deny credit to women and rural citizens, a risk it calls algorithmic apartheid.

The Strategy is nonetheless silent on TFGBV. Deepfakes appear twice, once as a misinformation threat to social trust, stability and democratic institutions and once as a reputational risk capable of eroding public confidence in AI. In neither instance are they recognised as instruments of sexual abuse, although non-consensual synthetic intimate imagery is among their most prevalent uses against women worldwide. Online violence against women is absent from the risk matrix, the ethics framework and the key performance indicators. The framing is state-centric and system-centric, protecting institutions and public trust rather than the bodily and psychological integrity of women users. The Strategy does, however, create openings. It mandates ethical impact assessments for high-risk applications, bias testing, a right to human appeal and an AI ethics committee, and it commits Government to a National AI Act and a revision of the Cyber and Data Protection Act for AI-specific needs. Each of these mechanisms could carry gender-responsive content if the gender machinery engages the drafting process.

The National Child Online Protection Policy 2026-2030

Cabinet approved the National Child Online Protection Policy in June 2026 as the first dedicated national framework on online child safety. According to the official post-Cabinet briefing it responds to online sexual exploitation and abuse, cyberbullying, harmful content, grooming, sextortion and privacy violations and rests on nine strategic focus areas spanning institutional capacity, the legal and regulatory framework, prevention, response and support, technical control and corporate responsibility, education, awareness and research (Government of Zimbabwe, 2026b). It aligns child online safety with the Constitution and the Children's Act and creates a coordinated framework involving government, the private sector, academia and communities.

The policy matters here because several of the harms it names are core forms of TFGBV as experienced by girls. Grooming and sextortion are gendered in their incidence and their recognition is a genuine advance on the gender-silent statutes reviewed above. Two observations follow, offered as a preliminary reading pending release of the full text. The first is that the framing appears age-based rather than gender-responsive, since girls are protected as children and the gendered patterning of the harms is not named. The second is a continuity problem. A girl groomed or sextorted at seventeen falls within the policy's protective framework while the same woman at eighteen falls into the legislative gap this paper maps. Protection ends precisely where the majority of TFGBV begins. The coordination architecture could nonetheless be extended toward adult women at limited marginal cost.

Table 2 summarises the assessment of all nine instruments.

Table 2. Assessment of the nine instruments against the four criteria

Instrument	Gendered harm recognised	Digital offences covered	Enforcement and survivor support	Coordination assigned
Constitution (2013)	No	No, silent on digital rights	General rights only	Commissions, not for online harm
Domestic Violence Act (2006)	Partial, GBV but not digital form	No	Orders do not reach online conduct	Offline actors only
Criminal Law Code (host statute, as amended 2021)	No	Hosts ss 164A to 164G; deepfakes fall between ss 164C and 164E	No digital forensic mandate	None specified
Cyber and Data Protection Act (2021)	No, gender unnamed in every	ss 164A, 164B, 164C, 164E; no AI-enabled	Punitive, no takedown or	Undefined across the three

	provision	abuse	survivor route	bodies
National Gender Policy (2025)	No, TFGBV undefined	No	Commitment without digital guidance	Stated, no TFGBV mechanism
National ICT Policy (2022-2027)	No	No	Infrastructure focus, no redress	Cybersecurity structures only
POTRAZ Child Online Protection Guidelines (2015)	No, gender-neutral	Partial, children only	Educational referral only	Limited
National AI Strategy (2026-2030)	Partial, inclusion and bias only	Deepfakes as misinformation risk only	Impact assessments, not survivor-centred	Ethics committee, no gender link
National Child Online Protection Policy (2026-2030)	Partial, framed by age	Yes for minors	Support mechanisms for children	Nine-part, ends at majority

Note. The Cyber and Data Protection Act amended sections 162 to 166 of the Criminal Law (Codification and Reform) Act. The two rows are assessed as drafting vehicle and host statute rather than as independent instruments. Cyber-bullying (sec 164B) carries up to ten years, non-consensual recording (sec 164A) up to five.

Interview findings

Adequacy of existing legal frameworks

Respondents consistently described the legal landscape as offering partial but fragmented protection. The Cyber and Data Protection Act was recognised as a milestone on offences such as cyber harassment, hacking and unlawful data disclosure, yet its orientation toward data systems leaves the gendered texture of online abuse unaddressed. A legal officer in the justice ministry (P1) observed

“The Cyber Act largely protects the integrity of data systems, not necessarily to respond to gender-based violence in digital spaces. Its scope is limited to criminalisation without a survivor-centred approach.”

The Domestic Violence Act and the Criminal Law Code were described as foundational but outdated. A survivor support practitioner (P6) explained that survivors must fit their cases into statutes never designed for digital abuse, while a coalition respondent (P8) reported that police often do not know under which Act to proceed and treat such reports as social matters requiring counselling, so cases fall away before prosecution. Participants also stressed inconsistency across statutes. A women's rights lawyer (P10) put it this way

“What we see is a real disconnect between the Cyber and Data Protection Act and the Domestic Violence Act. They sit in different ministries, speak different legal languages, and operate as if the harms they address were unrelated. Yet for the survivor, it's the same violence, only that it happens through a phone or computer instead of a fist.”

Gender sensitivity and conceptual recognition

Although national policies mention women's empowerment through ICTs, respondents noted that none had been designed around online abuse. An international gender specialist (P13) described gender as an add-on in digital policy, present as awareness that women face online abuse but absent from design. The absence of gender-disaggregated data reinforces this invisibility. A data analyst (P12) explained

“There is no systematic way of collecting and publishing data on online gender-based violence. Without gender-disaggregated statistics, policymakers continue to underestimate the scale of the problem because what is not counted is simply not seen.”

Two mechanisms sustain that invisibility. A women's rights lawyer (P11) linked underreporting to institutional attitudes, noting that survivors expect police to dismiss the matter as a lovers' quarrel. A practitioner (P7) identified misclassification, explaining that non-consensual sharing of intimate images is rarely recorded as gender-based violence and is logged instead as general cybercrime, which masks the gendered nature of the harm. A coalition respondent (P8) captured the chilling effect, observing that technology was meant to give women a voice but without protection has become another weapon against them.

Institutional coordination and enforcement

Responsibility for TFGBV is spread across the ICT ministry, the ministry responsible for women's affairs, POTRAZ, the Zimbabwe Republic Police, the Gender Commission and the Human Rights Commission, with overlapping mandates and no dedicated inter-ministerial mechanism. An ICT ministry official (P2) conceded

“We don't yet have a coordinated system that brings together ICT, gender, justice, and law enforcement to address online violence. Each ministry works in its silo, so the response is fragmented and inconsistent.”

Capability gaps mirror the mandate gaps and run in both directions. A practitioner (P6) observed that POTRAZ runs strong awareness campaigns but has no gender or psychosocial specialists able to support survivors, while a women's rights lawyer (P10) described the converse gap in the ministry responsible for women's affairs, which lacks the tools to monitor online spaces or engage platforms. Law enforcement capacity emerged as the weakest link. A Victim Friendly Unit officer (P4) explained

“Our police officers are still learning how to handle cyber-related cases. Most don't have digital forensic training or the equipment to trace offenders. So even when survivors report, the evidence at times gets lost or mishandled.”

A second officer (P5) confirmed that many reports die at the reporting stage for want of investigative tools.

Awareness, reporting and digital literacy

Low digital literacy among both the public and institutions emerged as a recurring barrier. Many survivors do not recognise coercive sexting, digital stalking or image-based abuse as violence, while others fear stigma or doubt police will act. A data analyst (P12) argued that without state leadership in public education and law enforcement training the work of civil society remains localised. A coalition respondent (P8) observed that journalists, politicians and activists are attacked more viciously precisely because they are visible, with the abuse intended to push them out of digital spaces. A women's rights lawyer (P10) described the rural dimension

“In rural areas, women face a double barrier. They lack digital literacy and access to safe online platforms. So when abuse happens, they don't even know how to report it or preserve evidence. Their silence is not consent, it's exclusion.”

Institutional and cultural barriers to justice

Interviewees consistently pointed to socio-cultural attitudes that trivialise digital abuse. A practitioner (P7) described a persistent perception that online abuse is not real violence, met with advice to block or ignore rather than recognition of psychological harm, while the gender specialist (P13) linked victim-blaming to evidentiary practice, describing a community belief that women invite abuse by being outspoken and a justice system built around physical evidence. Moralistic policing of women's online presence extends into law enforcement, as a coalition respondent (P9) recounted

“When a woman reports online abuse, the first question is often, ‘Why were you online?’ This reflects a moralistic policing of women’s presence in digital spaces.”

Emerging opportunities and prospects for reform

Respondents also identified openings for reform. At the time of the interviews the AI Strategy was awaiting launch and respondent P2 saw it as a chance to build safeguards in from the start

“The forthcoming AI policy gives us a real chance to embed gender-sensitive safeguards from the start. If we integrate principles of online safety and digital ethics into that framework, we can prevent technology from reproducing the same inequalities we’re trying to solve.”

The Strategy has since been launched and the opportunity was only partially taken. Gender enters as a matter of inclusion and bias but online violence against women is not named, which places the burden of gender-responsive implementation on the ethics and legislative mechanisms the Strategy creates. A police respondent (P5) argued that decentralising the national cyber laboratory beyond Harare would let survivors in rural areas have cases processed without travelling long distances.

Alternative perspectives

Government and law enforcement participants viewed the legislation as an important milestone in responding to cyber-enabled offences, arguing that recent arrests and prosecutions demonstrate that the law is operational and capable of addressing online misconduct. Publicly reported prosecutions under the cyber-bullying provisions, including cases involving social media personalities and other high-profile online users, were seen as evidence that the legal framework is increasingly being enforced. From this perspective, the principal challenge lies not in the absence of legislation but in improving implementation and institutional capacity.

There are a number of cases that have gone through the courts where people have been arrested, prosecuted, and some even convicted for TFGBV. A case in point is that of Mai Titi’s daughter and the case of Zodwa Mkandla

This perspective is consistent with publicly reported prosecutions under section 164B of the Criminal Law (Codification and Reform) Act, including the conviction arising from the TikTok cyberbullying case involving businesswoman Zodwa Mkandla and the prosecution of social media personality Ashley Jeke.

Those expressing this view therefore maintained that the priority should not necessarily be the enactment of additional legislation but rather the effective implementation of existing laws through enhanced public awareness, institutional coordination, digital forensic capacity and specialised training for law enforcement and judicial officers. In their assessment, Zimbabwe’s challenge is less one of legislative deficiency than of ensuring consistent enforcement, improved institutional capacity and greater public understanding of the legal remedies already available to survivors of technology-facilitated abuse.

DISCUSSION

The findings affirm the central claim of feminist legal theory that law, though formally neutral, is structured around male norms and responds poorly to women’s lived realities. The cyber provisions treat offences as technological breaches rather than violations of bodily integrity, a reductionism mirroring the public-private divide through which harms in non-physical spaces are minimised (Gilman, 2023, Wodajo, 2022). The refusal to define TFGBV as a distinct form of GBV reveals how law perpetuates hierarchy while claiming neutrality.

The new instruments extend rather than interrupt this pattern. The AI Strategy shows that Zimbabwean policymakers can now name algorithmic discrimination against women in credit and services, yet the same document discusses deepfakes solely as threats to the state, to elections and to public trust. Danger to institutions is legible where danger to women’s bodies is not. What the doctrinal analysis adds is that this selective legibility operates at three levels rather than one. It appears in policy language, where violence against women goes unnamed. It appears in the statute, where the tariff for reputational humiliation is double

that for non-consensual recording of the body. And it appears in enforcement, where the reported prosecutions cluster on the provision protecting reputation. Text, sentencing tariff and practice rank the same way, which makes the claim considerably harder to attribute to drafting oversight. It also shows that gender mainstreaming in distributional terms can coexist with gender blindness toward violence. The Child Online Protection Policy makes grooming and sextortion visible but only within the category of childhood, so protection expires at the age of majority. Together the two instruments confirm that the problem is not an absence of policy activity but the conceptual frame within which activity occurs.

The critique therefore calls for substantive rather than formal equality, since gender-neutral legal language perpetuates inequality when it ignores the different ways men and women experience violence. The interview data show a digital environment that, while expanding expression and connectivity, has become a terrain of control in which women journalists, activists and young professionals self-censor or withdraw (Mtero et al., 2023). This echoes scholarship reading TFGBV as digital patriarchy in which technology amplifies rather than dismantles gendered power (Henry and Powell, 2018; Masunda, 2024). The penalty structure permits a more precise diagnosis than the familiar charge of technocracy. The state does not disregard dignity. It ranks it, placing dignity as reputation above dignity as bodily integrity, and the ranking is legible in years of imprisonment rather than in rhetoric (Suzor et al., 2018, Mhajne and Whetstone, 2024).

This finding complicates the reform agenda rather than simplifying it. If the most actively used cyber provision is one that shields complainants with public standing, and if the accused in the reported cases are predominantly women, then a call for more criminal provisions is not straightforwardly protective. Feminist scholarship has long warned that criminal justice responses to technology-facilitated abuse fall hardest on marginalised communities and can be turned against the people they were meant to serve (Bailey, Flynn and Henry, 2021). Zimbabwe now supplies an illustration. The task is therefore rebalancing rather than expansion, correcting a tariff that already treats sexual autonomy as the lesser interest before adding further offences to a framework that misprices the ones it has.

Ubuntu and the limits of relational ethics

An unexplored resource for closing the gap lies in the AI Strategy's own ethical vocabulary. The Strategy grounds itself in Ubuntu, the principle that a person is a person through other persons. Read seriously, that commitment supplies a strong indigenous argument against image-based abuse and synthetic sexual imagery. Such harms do not merely injure an individual, they sever the relational bonds through which personhood is constituted, exposing a woman to her community in terms she did not choose. On its own terms Ubuntu should treat this as a grave wrong.

The Strategy does not draw that conclusion, and the reason is instructive. Absent an explicit feminist reading, communitarian ethics can default to protecting the community's institutions rather than its most exposed members. Dignity becomes public trust and relational harm becomes reputational risk to the state. The sentencing tariff is that default rendered in years. The treatment of deepfakes illustrates the default exactly. They threaten social stability and confidence in AI, and the woman whose likeness is used is not in the frame. A feminist reading of Ubuntu would invert that ordering and give Zimbabwean policymakers a vocabulary for gender-responsive digital governance that is neither borrowed from the Global North nor vulnerable to dismissal as foreign.

Intersectional analysis reveals who bears the heaviest burden. Urban women with public profiles are targeted through trolling and image-based violence while rural women are excluded from digital safety discourse by connectivity and literacy gaps. This reproduces intersectional invisibility in which some women's experiences fall outside both legal attention and mainstream advocacy (Crenshaw, 1989, Coles and Pasek, 2020).

Institutional weakness and cultural norms intersect to sustain TFGBV. Gender expertise is marginal in ICT governance, reflecting a bureaucratic logic in which cybersecurity is masculinised as hard policy while gender is feminised and underfunded. Police and judicial officers lack training on digital gender violence, and reliance on physical evidence disadvantages survivors of non-physical harm. This inertia undermines Zimbabwe's

commitments under Resolution 522 and the Malabo Convention, and closing the gap requires institutional reform and a cultural shift, not merely legal amendment.

RECOMMENDATIONS

The findings support a multi-sectoral framework linking ICT policy, the national gender machinery and survivor-centred support. Six measures follow, sequenced deliberately. The first two are legislative and time-bound, the third and fourth institutional and parallel, and the last two depend on the definitional work the first two accomplish.

First and most urgent, the revision of the Cyber and Data Protection Act mandated by the AI Strategy should be treated as the immediate legislative window, since it is the one reform with a government commitment and a timetable already attached. Responsibility rests with the ministry responsible for ICT as drafting lead, with the ministry responsible for women's affairs and the Zimbabwe Gender Commission brought into the drafting process rather than consulted after it. The first task is rebalancing rather than addition. The penalties attaching to non-consensual recording and to transmission of intimate images should be aligned with those for cyber-bullying, since the present ordering signals that sexual autonomy is the lesser interest. Beyond that, provisions are needed for deepfakes and other non-consensual synthetic intimate imagery, survivor-centred reporting, expedited content removal and duties of cooperation on platforms operating in Zimbabwe.

Second, the Domestic Violence Act should be amended to define TFGBV and to extend protection orders to online conduct, with responsibility resting on the ministry responsible for justice. Sequencing this after the Cyber Act revision allows the two statutes to share a single definition rather than generating a third inconsistent one.

Third, an inter-ministerial coordination mechanism on technology-facilitated violence should be established, drawing together the ministries responsible for ICT, women's affairs and justice with POTRAZ, the police and the Gender Commission. The AI Strategy's governance architecture and the coordination model of the Child Online Protection Policy provide ready templates, and gender expertise should be built into the planned AI ethics committee.

Fourth, enforcement capacity should be decentralised and professionalised through provincial cyber forensic laboratories, digital evidence training for Victim Friendly Units and procedures that protect survivors during investigation. Responsibility rests with the police in partnership with POTRAZ. Respondents identified this as the single change with the largest practical effect on rural access.

Fifth, gender-disaggregated data protocols should be adopted so that police recording standards and national statistics capture TFGBV as a category, with indicators written into the monitoring frameworks of the Gender Policy and the AI Strategy and the national statistics agency and Gender Commission jointly accountable.

Sixth, prevention and support should be survivor-centred and intersectionally designed, using local languages, community structures and mobile reporting channels that reach rural women, and the coordination architecture of the Child Online Protection Policy should be extended so that protection does not expire at the age of majority.

CONCLUSION

On the first research question the documentary analysis shows that the framework, now nine instruments deep, addresses aspects of digital safety but does not recognise TFGBV as a gendered harm. The Cyber and Data Protection Act criminalises without a survivor-centred approach, the Domestic Violence Act predates the digital era, the Gender and ICT policies are silent on online violence and the newest instruments repeat the pattern in updated form. The AI Strategy sees deepfakes as threats to the state but not to women, and the Child Online Protection Policy, on the material so far released, protects girls only until they become women. On the second question the interviews demonstrate that fragmentation across ministries, thin forensic capacity, absent data and cultural attitudes that trivialise online abuse combine to deny survivors effective redress. Enforcement

is nonetheless better described as selective than as weak, since the provision protecting reputation is actively prosecuted while those protecting sexual autonomy appear unused. On the third the analysis identifies concrete reform openings, chief among them the revision of the Cyber and Data Protection Act mandated by the AI Strategy, the planned National AI Act, decentralisation of forensic capacity and the coordination architectures created by the two 2026 instruments.

The persistence of these gaps reflects the patriarchal structure of a legal order that treats online violence as a technical or moral problem rather than a manifestation of systemic inequality. The Strategy's own Ubuntu vocabulary offers an indigenous foundation for a different approach, provided it is read to protect the most exposed members of the community rather than the standing of its institutions. Adequacy should be measured not by the existence of laws but by their capacity to transform power relations and secure justice for survivors.

The study has limitations. The sample comprised thirteen institutional informants and excluded survivors, whose experiences of seeking redress warrant dedicated research under appropriate ethical safeguards. The Child Online Protection Policy was assessed from its official summary and that assessment should be revisited once the full text is published. The observations on enforcement rest on reported cases in the media rather than on court records or prosecution statistics, and are offered as indicative rather than as a caseload analysis. The analysis reflects the position as at mid-2026. Future research should examine implementation of the AI Strategy's ethics mechanisms from a gender perspective, track prosecutions under the Cyber and Data Protection Act using the disaggregated data this paper calls for and centre survivors' own accounts.

DISCLOSURE

There are no relevant financial or non-financial competing interests to report.

REFERENCES

1. Abdulquadir, A. (2020). Regional trade and the challenges of data protection in West Africa. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.3770159>
2. Abdulrauf, L. A. and Fombad, C. M. (2016). The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa? *Journal of Media Law*, 8(1), 67-97. <https://doi.org/10.1080/17577632.2016.1183283>
3. African Commission on Human and Peoples' Rights (2022). Resolution 522 on the Protection of Women against Digital Violence in Africa. Banjul, ACHPR.
4. Bailey, J., Flynn, A. and Henry, N. (Eds.) (2021). *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Bingley, Emerald Publishing. <https://doi.org/10.1108/9781839828485>
5. Bande, L. C. (2023). ICTs, crime and human rights. In Chirwa, D. and Ncube, C. (Eds.), *The Internet, Development, Human Rights and the Law in Africa*. London, Routledge.
6. Bansal, V., Leasure, E., Roth, C., Rezwan, M., Iyer, M., Pal, P. and Hinson, L. (2022). Help-seeking behaviours of those experiencing technology-facilitated GBV in Asia: implications for policy and programming. *Journal of Gender-Based Violence*, 7(2), 352-363. <https://doi.org/10.1332/239868021x16697232129517>
7. Bengesai, A. V. and Chikhungu, L. (2025). Violence against women and girls in Zimbabwe: a review of a decade of the empirical literature. *Trauma, Violence & Abuse*, 26(4), 769-788. <https://doi.org/10.1177/15248380241291074>
8. Boshe, P., Hennemann, M. and von Meding, R. (2022). African data protection laws: current regulatory approaches, policy initiatives, and the way forward. *Global Privacy Law Review*, 3(2), 56-88. <https://doi.org/10.54648/gplr2022008>
9. Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. <https://doi.org/10.1191/1478088706qp063oa>
10. Citron, D. K. (2014). *Hate Crimes in Cyberspace*. Cambridge MA, Harvard University Press.
11. Coles, S. M. and Pasek, J. (2020). Intersectional invisibility revisited: how group prototypes lead to the erasure and exclusion of Black women. *Translational Issues in Psychological Science*, 6(4), 314-324. <https://doi.org/10.1037/tps0000256>
12. Constitution of Zimbabwe Amendment (No. 20) Act (2013). Harare, Government of Zimbabwe.

13. Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: a Black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum*, 1989(1), 139-167.
14. Criminal Law (Codification and Reform) Act [Chapter 9:23] (2004). Harare, Government of Zimbabwe.
15. Cyber and Data Protection Act [Chapter 12:07] (2021). Harare, Government of Zimbabwe.
16. Domestic Violence Act [Chapter 5:16] (2006). Harare, Government of Zimbabwe.
17. Dragiewicz, M., Burgess, J., Matamoros-Fernandez, A., Salter, M., Suzor, N. P., Woodlock, D. and Harris, B. (2018). Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, 18(4), 609-625.
<https://doi.org/10.1080/14680777.2018.1447341>
18. Dunn, S. (2021). Is it actual violence? Framing technology-facilitated abuse as violence. In Bailey, J., Flynn, A. and Henry, N. (Eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Bingley, Emerald Publishing.
19. Esposito, E. and Semenzin, S. (2025). Women's activism online in Italy: claiming spaces, navigating misogyny, reimagining feminisms. *European Journal of Communication*.
<https://doi.org/10.1177/02673231251349009>
20. Gilman, M. E. (2023). Feminism, privacy and law in cyberspace. In Brake, D., Chamallas, M. and Williams, V. L. (Eds.), *The Oxford Handbook of Feminism and Law in the United States*. New York, Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780197519998.013.36>
21. Government of Zimbabwe (2022). Zimbabwe National ICT Policy 2022-2027. Harare, Ministry of Information Communication Technology, Postal and Courier Services.
22. Government of Zimbabwe (2026a). Zimbabwe National Artificial Intelligence Strategy 2026-2030. Harare, Ministry of Information Communication Technology, Postal and Courier Services.
23. Government of Zimbabwe (2026b). Zimbabwe National Child Online Protection Policy 2026-2030. Harare, Government of Zimbabwe.
24. Greenleaf, G. and Cottier, B. (2021). International and regional commitments in African data privacy laws: a comparative analysis. *Computer Law & Security Review*, 44, 105638.
<https://doi.org/10.1016/j.clsr.2021.105638>
25. Harris, B. A. and Woodlock, D. (2019). Digital coercive control: insights from two landmark domestic violence studies. *The British Journal of Criminology*, 59(3), 530-550.
<https://doi.org/10.1093/bjc/azy052>
26. Henry, N. and Powell, A. (2015). Embodied harms: gender, shame, and technology-facilitated sexual violence. *Violence Against Women*, 21(6), 758-779. <https://doi.org/10.1177/1077801215576581>
27. Henry, N. and Powell, A. (2018). Technology-facilitated sexual violence: a literature review of empirical research. *Trauma, Violence & Abuse*, 19(2), 195-208.
<https://doi.org/10.1177/1524838016650189>
28. Jane, E. A. (2017). *Misogyny Online: A Short (and Brutish) History*. London, Sage.
29. Makulilo, A. B. (2015). Myth and reality of harmonisation of data privacy policies in Africa. *Computer Law & Security Review*, 31(1), 78-89. <https://doi.org/10.1016/j.clsr.2014.11.005>
30. Masunda, O. (2024). Peace Education 4.0: A Curriculum Framework for Africa. *Academia Lasalliana Journal of Education and Humanities*, 6(1). <https://doi.org/10.55902/SJCE7127>
31. Mhajne, A. and Whetstone, C. (2024). A feminist cybersecurity: addressing the crisis of cyber(in)security. *International Affairs*, 100(6), 2341-2360. <https://doi.org/10.1093/ia/iaae234>
32. Ministry of Women Affairs, Gender and Community Development (2025). *National Gender Policy*. Harare, Government of Zimbabwe.
33. Mtero, S., Parichi, M. and Madsen, D. H. (2023). Patriarchal politics, online violence and silenced voices: the decline of women in politics in Zimbabwe. *Strategic Review for Southern Africa*, 45(2).
<https://doi.org/10.35293/srsa.v45i2.4970>
34. Orji, U. J. (2018). The African Union Convention on Cybersecurity: a regional response towards cyber stability? *Masaryk University Journal of Law and Technology*, 12(2), 91-130.
<https://doi.org/10.5817/mujlt2018-2-1>
35. Plan International (2020). *Free to Be Online? Girls' and Young Women's Experiences of Online Harassment*. Woking, Plan International.

36. POTRAZ (2015). Child Online Protection Guidelines for Children. Harare, Postal and Telecommunications Regulatory Authority of Zimbabwe.
37. Powell, A. and Henry, N. (2017). Sexual Violence in a Digital Age. London, Palgrave Macmillan.
38. Sutherland, E. (2018). Digital privacy in Africa: cybersecurity, data protection and surveillance. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.3201310>
39. Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J. and Van Geelen, T. (2018). Human rights by design: the responsibilities of social media platforms to address gender-based violence online. *Policy & Internet*, 11(1), 84-103. <https://doi.org/10.1002/poi3.185>
40. UN Women (2022). Accelerating Efforts to Tackle Online and Technology-Facilitated Violence against Women and Girls. New York, UN Women.
41. Wodajo, K. (2022). Mapping (in)visibility and structural injustice in the digital space. *Journal of Responsible Technology*, 9, 100024. <https://doi.org/10.1016/j.jrt.2022.100024>
42. Yardley, E. (2021). Technology-facilitated domestic abuse in political economy: a new theoretical framework. *Violence Against Women*, 27(10), 1479-1498. <https://doi.org/10.1177/1077801220947172>
43. Zindi, P., Amadhila, H., George, F., Acheampong, M. and Mwamba, K. (2025). Digital inclusion and social inequality: gender differences in ICT access and use in Harare. *International Journal for Multidisciplinary Research*, 7(5). <https://doi.org/10.36948/ijfmr.2025.v07i05.53062>
44. Zirima, P. and Sithole, S. (2025). Understanding Technology-Facilitated Gender-Based Violence (TFGBV) against Women Journalists in Zimbabwe. Harare, Gender and Media Connect and UNESCO.