Online challenges, offline realities:

A feminist analysis of women human rights defenders' digital experiences

RESEARCH REPORT – TRENDS AND TACTICS

ONLINE CHALLENGES, OFFLINE REALITIES:

A feminist analysis of women human rights defenders' digital experiences

Research
Anaís Córdova-Páez

Additional research and editing
Islam Al-Khatib

Reviewers
Carla Vitoria Barbosa (APC)
Hija Kamran (APC)
Sadaf Khan (APC)

Copy editing
Islam Al Khatib

Proofreading
Lynne Stuart

Design and layout
Sahar Khan

Production
Carla Vitoria (APC)

Support
Cathy Chen (APC)
Lori Nordstrom (APC)
Shamiso Mahomva (APC)

Published by the Association for Progressive Communications (APC), 2025

ISBN 978-92-95113-73-2
APC-202509-SFV-R-EN-DIGITAL-363

Table of contents

INTRODUCTION

Digital networks have become a battleground where hegemonic power is both consolidated and challenged. As governments, corporations and Big Tech assert control over online spaces, the internet, once imagined as a space for free expression, has increasingly become a tool for surveillance, censorship and repression. This shift, often described as digital authoritarianism, has profound consequences for women human rights defenders (WHRDs), whose work disrupts entrenched power structures and exposes them to unique forms of online violence.

The erosion of democratic principles and the rise of digital repression go hand in hand. Institutional frameworks and political and economic development in Global South countries are shaped by colonial legacies that give rise to digital authoritarianism, which does not operate in isolation. It is deeply entangled with offline political dynamics, reinforcing state and corporate control and shrinking civic space in ways that exhibit a distinctly patriarchal approach to violence. Through surveillance laws, content moderation policies and internet shutdowns, governments and tech companies justify the silencing of dissent while shielding themselves from accountability. The six countries examined in this research, i.e. Brazil, Ecuador, India, the Philippines, Uganda and Tanzania, vary in their democratic structures, yet share a common fragility in their institutions.

For WHRDs, the internet is both a vital space for resistance and a site of profound risk. It enables mobilisation, facilitates community building and allows for the articulation of feminist, environmental and human rights struggles across borders. Yet it also exposes them to relentless attacks: ranging from coordinated defamation and harassment campaigns to doxxing, stalking and threats of physical violence.

The current anti-rights backlash is deeply gendered. WHRDs are targeted not only for their activism but also for their identities, as women, queer individuals or gender-diverse people challenging patriarchal norms. The violence they face online functions as a mechanism of silencing, reinforcing broader systems of oppression.

This research situates digital violence in six countries within a Feminist Holistic Protection framework, as defined in the methodology section, recognising that threats against WHRDs are never isolated. The intersection of gender-based violence with digital repression amplifies existing inequalities, making it harder for WHRDs to counter violence or access justice. At the same time, technological advancements combine with evolving state and corporate repression to constantly reshape the digital landscape, creating new risks that outpace existing rights-protecting responses.

Through an analysis of legal frameworks and WHRDs' experiences in Brazil, Ecuador, India, the Philippines, Uganda and Tanzania, this research explores the interconnection between technology-facilitated gender-based violence (TFGBV) and digital authoritarianism, highlighting the ways activists resist, adapt and reclaim space amid escalating online and offline threats.

The findings reveal several key trends:

- The weaponisation of gender, bodies and sexuality as primary sites of attack, with WHRDs facing misogynistic rhetoric and online abuse that reinforce patriarchal and conservative ideologies.

- A continuum between online violence and offline repression, where tactics like doxxing, smear campaigns and surveillance escalate into physical threats, arrests and even assassination attempts, all exacerbated by the failure to implement or establish rapid response protection mechanisms.

- Structural discrimination embedded in technology, with racialised, Indigenous and marginalised WHRDs disproportionately targeted through algorithmic bias, state surveillance and exclusion from digital security frameworks.

- The weaponisation of legal systems to criminalise dissent, using anti-terrorism, cybercrime and morality laws to silence WHRDs, alongside financial repression tactics that restrict funding and operational capacity.

- The unrestrained expansion of surveillance, with spyware, biometric tracking and facial recognition technologies deployed under the guise of security, intensifying repression.

- The intersection of digital authoritarianism and extractivism, where both natural resources and personal data are exploited to consolidate power, with Indigenous land defenders facing heightened risks.

WHRDs across the six countries have urged governments to implement gender-sensitive cybersecurity laws that explicitly address digital violence and to establish holistic, rapid response mechanisms to prevent escalation. Special attention must be given to grassroots, Indigenous and rural WHRDs, who face disproportionate, multi-layered risks. Accountability for Big Tech requires an effective governance model and stronger policy enforcement by social media companies such as Meta and X (formerly Twitter) to curb digital violence, censorship and the proliferation of hate speech globally.

Safeguards against state surveillance must also be enforced to prevent misuse under national security pretexts, ensuring judicial oversight and proportionality. Combating disinformation through robust fact-checking initiatives is crucial to dismantling smear campaigns that put WHRDs and marginalised communities at risk.

This research highlights the urgent need for systemic change, not only in policies and legal frameworks, but also in the underlying structures that enable digital and physical violence against WHRDs around the world.

METHODOLOGY

The research followed a feminist methodology committed to producing socially just, transformative and empowering knowledge. This approach explicitly prioritised care, safety and the well-being of participants throughout the research process. In designing interview questionnaires and focus group discussions, careful attention was paid to the language used, ensuring it was accessible, inclusive and free from overly technical jargon. Tech-specific terms were clearly explained, and questions were framed in an open-ended, non-leading manner to enable genuine and safe engagement.

Recognising the varied backgrounds and differing degrees of technological familiarity among participants, all interviews and focus group discussions were conducted by national and local researchers. Their contextual knowledge and cultural familiarity helped foster trust and facilitated deeper understanding, particularly when working with rural, Indigenous and Quilombola WHRDs in remote areas. To ensure these groups were not excluded, interviews were also conducted by phone.

Given the potential emotional distress that could arise when discussing traumatic experiences of violence, the research process included clear trigger warnings. Researchers were trained to approach sensitive topics with empathy and care, allowing participants to engage at their own comfort levels, pause interviews or choose not to respond to certain questions.

Intersectionality was central to the methodology, acknowledging that violence is shaped by the intersections of race, class, caste, disability, gender identity and other social markers. This framing allowed the research to document nuanced experiences and offer a more holistic analysis of the impacts on WHRDs' lives and activism.

The countries were selected based on the Safety for Voices consortium's geographic diversity across the Global South and the presence of strong local networks and established partnerships with APC member organisations. The differences in cultural and legal frameworks, as well as policy environments across the six countries, offered a rich basis for comparative analysis of digital safety and security practices for WHRDs. Local researchers and partner networks ensured that WHRDs' experiences were interpreted within the specific contexts of each country.

- Uganda and Tanzania (East Africa) have active WHRD movements and broader human rights communities but operate under increasingly restrictive legal frameworks that criminalise dissent.

- India and the Philippines (South and Southeast Asia) have strong feminist and civil society organising for gender justice, but both have witnessed democratic erosion, the expansion of digital surveillance and the repression of activism.

- Brazil and Ecuador (South America) host powerful WHRD movements, especially in land defence and environmental justice, yet defenders face rising levels of physical and digital violence from both state and corporate actors.

Feminist Holistic Protection

The Feminist Holistic Protection (FHP) framework integrates multiple dimensions of care, understanding that digital care is intertwined with the physical, institutional/judicial, well-being and collective dimensions.

It aims to enhance the safety, well-being and agency of women human rights defenders through an intersectional approach. FHP recognises that structural inequalities, such as sexism, racism and economic disparities, are deeply connected to the threats individuals face. Therefore, in order to advocate for sustainable security, it is crucial to address these root causes.

The digital landscape and access to technology vary significantly across these countries. This research does not aim to generalise findings across all Global South contexts. Instead, it focuses on identifying patterns within specific national environments, with careful attention to the intersectional factors that shape WHRDs' experiences of digital repression. Social and cultural dynamics remain central to understanding how gender, race, class and other identities mediate risk.

The research assessed trends in recent years across six thematic areas of legal enforcement and policy implementation:

- Online surveillance and data protection
- Cyber harassment and online threats
- Freedom of expression and access to information
- Freedom of association and assembly
- Incitement to violence and hate speech regulations
- Technology-facilitated gender-based violence.

Drawing on legal frameworks, case law and precedents, the study examines how these intersecting domains affect WHRDs' safety, activism and access to justice. The findings highlight gaps in protection and provide concrete recommendations for legislative reforms that better secure WHRDs' digital rights.

Approximately 10 in-depth interviews were conducted per country with WHRDs and experts in digital rights, feminist activism and human rights. These interviews captured direct testimonies of digital violence, strategies for resilience and the varied responses of states and corporations to online threats. All interviews were carried out with informed consent and robust safety protocols, ensuring anonymity and minimising risk to participants.

In addition to individual interviews, focus group discussions were convened in each country. These collective spaces enabled WHRDs to reflect on shared experiences, validate emerging findings and elaborate on key insights. Country researchers led the identification of participants, ensuring thematic and geographic diversity. A strong emphasis was placed on intersectionality in participant selection, with attention to defenders working across a wide range of movements and issues, including:

- Feminist activism and gender justice
- Digital rights and freedom of expression
- Land, environmental and Indigenous sovereignty
- Disability justice
- LGBTQIA+ rights
- Prison abolition and criminal justice reform
- Anti-caste struggle
- Anti-racism and Black women’s rights
- Reproductive rights and justice
- Migrant and refugee dignity
- Children’s and family rights
- Labour rights and worker protections
- Climate justice

CONTEXT OVERVIEW

The purpose of this section is to outline the relevant literature and empirical examples that inform the analytical framework of this research. This section does not aim to provide a comprehensive account of the overall digital and legal landscape across the six countries selected, nor does it claim to capture the full complexity of each national context. Rather, in the interest of clarity and analytical coherence, it offers a broad overview of the legal frameworks and online governance structures that shape the digital environments in which women human rights defenders operate.

While this general context provides a foundation for understanding regional trends, the specific impact of these policies on WHRDs varies significantly across national jurisdictions. Therefore, in the country-specific sections that follow, the report will examine in greater depth the legislative measures, regulatory practices and socio-political dynamics that directly influence the digital rights and security of WHRDs in each country.

Brazil and Ecuador

Brazil and Ecuador are both presidential republics with autonomous institutions and regular elections that operate under national legislatures and supreme courts, alongside specialised judicial bodies that oversee constitutional and electoral matters. Yet their legal and political foundations shape distinct landscapes for digital governance and human rights advocacy.

In Brazil, under Jair Bolsonaro's administration, the government leveraged intelligence tools for mass surveillance, tracking activists, journalists and political opponents. Legal battles between Big Tech and Brazilian authorities, exemplified by Elon Musk's dispute with the Supreme Court,[1] reflect broader tensions over misinformation regulation and digital platform accountability. Though Brazil reformed its outdated National Security Law, digital rights activists remain sceptical, especially given the current dispute over provisions targeting fake news dissemination.[2] Additionally, the General Data Protection Law was misused to restrict public access to information, a practice reversed in 2023 after the change in administration.[3]

---

1 Santos, S. F. (2024, 31 August). Musk's X banned in Brazil after disinformation row. *BBC News*. https://www.bbc.com/news/articles/c5y3rnl5qv3o

2 Human Rights Watch. (2020, 24 June). Brazil: Reject "Fake News" Bill. https://www.hrw.org/news/2020/06/24/brazil-reject-fake-news-bill

3 Borges de Carvalho, L. (2023). Data protection and public institutions in Brazil: new challenges, old administrative practices. *Administrative Law Review, 281*(1), 133-161.

At the same time, Brazilian law has increasingly addressed online crimes, including TFGBV, particularly those targeting marginalised groups. These measures reflect a growing recognition of the internet as a space where discrimination and violence occur, yet enforcement remains uneven, and concerns persist over how these legal mechanisms are applied in practice.

In Ecuador, digital rights protections exist in law but often conflict with security policies that grant unchecked digital surveillance to authorities, raising alarms about state overreach. Civil society organisations[4] warn that rushed policy making has enabled disproportionate surveillance without adequate safeguards.

Access to reliable information remains a contested issue across both contexts. While Ecuador's legal framework promotes media plurality and public access to government data, restrictive provisions criminalise whistleblowing and impose harsh penalties for unauthorised disclosures. Brazil's shifting legal landscape has similarly sparked debates over press freedom, online accountability, and the role of state oversight in digital communication.

India and the Philippines

India and the Philippines share complex legal frameworks that both protect and undermine digital rights, particularly for WHRDs. Both countries have

4 Association for Progressive Communications. (2022, 22 June). Civil society organisations reject attempts to silence and criminalise social movements in the context of protests in Ecuador and demand that human rights are respected. https://www.apc.org/en/pubs/civil-society-organisations-reject-attempts-silence-and-criminalise-social-movements-context

constitutions that enshrine fundamental rights, including freedom of expression and privacy, yet state surveillance, legal harassment and online abuse continue to constrain digital activism. As a result, WHRDs in both countries navigate increasingly hostile online environments shaped by state-led surveillance and the weaponisation of cyber laws.

In India, digital repression is reinforced through sweeping surveillance measures. The Telecommunications Act (2023) broadens state control over digital communications, while mass surveillance systems like NatGrid and the Pegasus spyware project have targeted activists, journalists and WHRDs.[5]

Similarly, in the Philippines, the expansion of state surveillance has restricted digital freedoms. The SIM Card Registration Act and the Philippine Identification System (PhilSys) create extensive databases of personal information, raising concerns about privacy violations and the increased targeting of activists. The Anti-Terrorism Act (ATA) further threatens WHRDs, enabling state authorities to monitor, red-tag and criminalise dissent under broad definitions of terrorism. Meanwhile, the Cybercrime Prevention Act imposes harsher penalties for crimes committed online, including cyber libel,[6] which has been used to silence WHRDs and journalists critical of the government.[7]

Legal provisions against online gender-based violence exist but are inconsistently enforced. The Safe Spaces Act criminalises online harassment, including cyberstalking, non-consensual sharing of intimate images and gender-based hate speech. The Anti-Photo and Video Voyeurism Act penalises unauthorised recording and distribution of intimate content, a tactic often used to intimidate WHRDs. However, while these laws acknowledge the digital threats faced by women, their enforcement remains selective, with state authorities more often deploying cyber laws to suppress activism than to protect those targeted by online violence.

---

5 Amnesty International. (2023, 31 March). India: Government's pursuit of new surveillance technology heightens human rights concerns. https://www.amnesty.org/en/latest/news/2023/03/india-governments-pursuit-of-new-surveillance-technology-heightens-human-rights-concerns/

6 Libel is penalised under Article 355 of the Revised Penal Code, and when committed online, it is classified as cyber libel under the Cybercrime Prevention Act (Republic Act No. 10175). Section 6 of this law increases the penalty for libel when committed through digital platforms, with imprisonment ranging from six to 12 years (prisión mayor).

7 Palatino, M. (2022, 25 February). Philippines's mandatory SIM card registration threatens privacy and free speech *The Diplomat*. https://thediplomat.com/2022/02/philippiness-mandatory-sim-card-registration-threatens-privacy-and-free-speech/

Uganda and Tanzania

Uganda and Tanzania share legal and political structures that regulate the digital sphere, shaping the conditions in which WHRDs operate online. Both countries have constitutional provisions that recognise fundamental rights, yet in practice, online spaces remain heavily surveilled and controlled through broad and often vaguely defined laws.

In Uganda, the Regulation of Interception of Communications Act (RICA) and the Anti-Terrorism Act enable extensive state surveillance, often in contradiction to constitutional privacy protections. Similarly, Tanzania lacks explicit safeguards against online surveillance, allowing state institutions to monitor and suppress dissent with little oversight. In both contexts, WHRDs, activists and civil society organisations face significant risks when engaging in digital advocacy, as online spaces are increasingly weaponised to silence political opposition and restrict gender justice activism.

The Ugandan government's reliance on digital repression is exemplified by the Computer Misuse Act (2011),[8] which has been used to arrest activists, journalists and political dissidents.[9] WHRDs and feminist activists have been particularly vulnerable to politically motivated cyber harassment, often perpetrated by state-aligned actors or influential public figures.

Self-censorship has become common among LGBTQIA+ activists due to the Anti-Homosexuality Act (2023), which criminalises the "promotion of homosexuality" through electronic communication, carrying severe penalties for individuals and organisations.[10] In recent years, opposition figures and environmental defenders, particularly those protesting the East African Crude Oil Pipeline (EACOP), have been targeted through a combination of online harassment, digital surveillance and direct state intimidation.[11]

---

8 Amnesty International. (2022, 14 October). Uganda: Scrap draconian law aimed at suppressing freedom of expression online. https://www.amnesty.org/en/latest/news/2022/10/uganda-scrap-draconian-law/

9 In a positive development, in January 2023 the Constitutional Court held that section 25 of the Computer Misuse Act was unjustifiable for being inconsistent with Article 29 of the Constitution regarding the protection of freedom of conscience, expression, movement, religion, assembly and association, and called for an immediate halt to its enforcement. Section 25 had provided that "any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor and is liable on conviction to a fine not exceeding twenty-four currency points or imprisonment not exceeding one year or both."

10 Human Rights Watch. (2024, 4 April). Uganda: Court upholds Anti-Homosexuality Act. https://www.hrw.org/news/2024/04/04/uganda-court-upholds-anti-homosexuality-act

11 StopEACOP. (2023, 7 December). EACOP: A trail of fear and intimidation for climate activists and land defenders. https://www.stopeacop.net/our-news/eacop-a-trail-of-fear-and-intimidation-for-climate-activists-and-land-defenders

Tanzania exhibits similar patterns of digital repression, where gender-based violence and online censorship intersect to limit WHRDs' ability to advocate for human rights. The Equality of Human Beings Act (1984) guarantees non-discrimination, yet gender-based violence remains widespread, particularly in rural areas where spousal violence affects over half of women.

> High rates of adolescent fertility suggest significant levels of unreported sexual violence, exacerbated by cultural stigma and legal barriers to justice. Without explicit legal protections against online surveillance, activists and WHRDs increasingly resort to pseudonymous accounts and encrypted communication to avoid state monitoring.

The use of social media by government institutions to track, intimidate and criminalise activists further restricts freedom of expression, with growing concerns about the unchecked expansion of digital surveillance in both Tanzania and Uganda.

In both countries, the legal and regulatory frameworks governing the digital sphere operate in ways that disproportionately impact WHRDs. While Uganda and Tanzania maintain constitutional commitments to equality and privacy, their broader legislative and enforcement practices allow for widespread state control over online spaces. This has created an environment where WHRDs must navigate constant threats of digital surveillance, cyber harassment and criminalisation, reinforcing the broader trends of state repression and gendered digital violence in the region.

KEY TRENDS

This research, grounded in an analysis of policy frameworks and the lived experiences of women and gender-diverse human rights defenders in Brazil, Ecuador, India, the Philippines, Uganda and Tanzania, reveals technology-facilitated violence as a tactic of repression, and examines the ways in which defenders resist, adapt and reclaim space. It traces the escalation of digital violence into offline threats, the weaponisation of surveillance technologies and legal frameworks to silence activists, and the persistent efforts of WHRDs to challenge these systems and seek justice across both online and offline domains.

Body and sexuality as the first frontier of attacks

Anti-rights movements exploit digital platforms to polarise public opinion, fuelling misogynistic rhetoric and positioning WHRDs as primary targets. Far-right groups use anti-feminist discourse to reinforce conservative ideologies, amplifying their influence and silencing defenders.

WHRDs are frequently attacked not only for their activism but for their gender, bodies and sexual identity.

> Interviewees reported receiving rape threats as retaliation for their work, reflecting how online violence mirrors entrenched patriarchal power structures. LGBTQIA+ WHRDs face heightened risks, including threats of corrective rape, particularly in India, Uganda, Ecuador and the Philippines.

The non-consensual sharing of intimate images, including deepfakes, is another tactic used to silence WHRDs, with victims blamed instead of perpetrators. In Uganda, laws such as the Anti-Pornography Act and the Computer Misuse Act have been weaponised against women, reinforcing institutional victim-blaming and deepening gender inequalities. Similarly, digital platforms' restrictions on sex work and trans rights fuel stigma and disinformation, further marginalising defenders.

Across Uganda, Ecuador and Brazil, violence against WHRDs advocating for reproductive rights and LGBTQIA+ issues is escalating. Uganda's Anti-Homosexuality Act criminalises not only LGBTQIA+ identities but also any form of advocacy or support, including receiving foreign funding. This law severely restricts WHRDs' ability to operate, tightening state control over civil society.

Gendered violence is not limited to right-wing spaces. Many WHRDs experience discrimination even in progressive circles, where their demands for rights are dismissed as "divisive". Meanwhile, AI-driven disinformation campaigns, including deepfake pornography and automated bot attacks, are increasingly used to discredit WHRDs. These technologies blur the line between reality and falsehood, making it harder for defenders to counteract attacks or seek justice.

Tactics also evolve to bypass content moderation. In India, perpetrators use vernacular language, blending Hindi and English to evade detection by AI-driven moderation systems. Words like "didi" (sister) are repurposed as insults against feminists, while religious slogans such as "Jai Shree Ram" (JSR) with a history of inciting violence, are used to intimidate WHRDs within the country's political context.[12] Despite claims of regional content moderation, which remains inadequate in the unique contexts of each country in the region, platforms fail to act, allowing targeted harassment to persist unchecked.

Digital repression and the online-to-offline violence continuum amid lack of platform accountability

As with all forms of TFGBV, online attacks against WHRDs rarely remain confined to digital spaces. They often escalate into offline threats, harassment and physical harm. Tactics such as doxxing, cyberstalking and smear campaigns increase activists' vulnerability to surveillance, arrest and direct violence. When personal information is leaked, WHRDs are not only compelled to self-censor, but also face in-person intimidation, workplace retaliation, coordinated assaults, death threats and, in extreme cases, assassination attempts.

These attacks tend to intensify during elections and moments of political crisis, including national strikes, states of emergency, carceral massacres, extractivist interventions and other periods of unrest. WHRDs mobilising against state repression, corporate abuse and systemic injustice are subjected to relentless online harassment, mass reporting and targeted digital surveillance, all tactics designed to discredit their work and suppress dissent.

Digital platforms have consistently failed to prevent or respond meaningfully to violence against activists. This failure stems from corporate decisions that prioritise profit over user safety and accessibility. Such neglect deepens the

12 BBC News. (2019, 10 July). Jai Shri Ram: The Hindu chant that became a murder cry. *BBC News*. https://www.bbc.com/news/world-asia-india-48882053

gender divide in technology and renders online spaces increasingly hostile to WHRDs. The removal of protective filters by Facebook (Meta) in January 2025 offers a stark example, enabling discriminatory discourse and hate speech to proliferate unchecked. Since the acquisition of Twitter (now X) by Elon Musk, reports of hate speech have surged, while mechanisms that previously addressed doxxing and harassment have become largely ineffective. Reports of abuse are frequently dismissed on the grounds that they "do not violate community guidelines," a loophole often exploited by perpetrators using region-specific or vernacular language to bypass moderation systems.

Structural discrimination in tech, including systemic racism and gender bias

The Global South is shaped by the enduring history of colonialism, which continues to define its sociopolitical and economic structures. In digital spaces, the rise of nationalist and xenophobic discourse disproportionately targets racialised women, exposing them to heightened levels of online violence.

Algorithmic bias reinforces these systemic inequalities, censoring content related to racial justice and activism while allowing hateful rhetoric to spread unchecked.

> Platforms frequently flag discussions by racialised individuals as hate speech, while failing to moderate actual hate-driven content. Beyond content moderation, algorithmic discrimination extends to surveillance practices, such as facial recognition technologies, which misidentify racialised individuals at alarmingly higher rates than white individuals, deepening structural oppression.

Indigenous defenders face persistent efforts to delegitimise their activism, often through attacks on their identity. In Brazil and Ecuador, Indigenous leaders are routinely accused of not being "Indigenous enough" to represent their communities, a tactic used to undermine their credibility and silence their advocacy. In India, caste and religious intolerance serve as powerful tools of exclusion, with WHRDs from marginalised castes facing relentless online violence.

The digital sphere, instead of being an equaliser, is a space where power imbalances are reinforced, and those fighting for justice are systematically silenced.

Digital inequality: Access, security and exclusion

The post-pandemic era has made the digital sphere critically important for the defence of rights and reshaped WHRDs' relationship with technology, compelling them to adapt, learn new tools and rely more on online spaces for advocacy. It has also made digital access gaps more glaring.

Lack of access and the digital divide remain more intense for rural WHRDs, who often must navigate a combination of digital illiteracy, high costs of internet access and equipment, and online threats such as smear campaigns that further discourage their participation in digital spaces. WHRDs with disabilities face even greater barriers in a context in which access to technology is essential for survival, daily interactions and political participation.

Language is another major barrier. Digital security curricula are often designed in technical, academic and Global North-centric language, excluding non-English speakers and activists whose realities are far removed from these frameworks. Many struggle to navigate security guides filled with jargon such as doxxing, stalking and phishing, making critical safety knowledge inaccessible.

The weaponisation of law: SLAPPs, criminalisation and financial repression

Access to justice remains a major hurdle for WHRDs, particularly due to the lack of understanding among judges, lawyers and other legal practitioners about digital rights, gender-based violence and the specific challenges faced by activists, including strategic lawsuits against public participation (SLAPPs) that are often used to silence WHRDs in public spheres. This gap in fair access to legal systems is especially evident in rural areas, where WHRDs encounter significant barriers at every stage of the legal process, from filing complaints to securing a fair verdict. Many interviewees expressed frustration at a system that often dismisses their cases, discouraging them from seeking justice.

One of the key tactics of digital authoritarianism is the misuse of judicial systems to silence WHRDs, often by perpetrators and sometimes by the state itself. This tactic gives a false appearance of legitimacy to actions meant to intimidate, criminalise and discredit defenders. Many interviewees reported facing defamation and slander lawsuits through SLAPPs, tactics frequently used to exploit gaps in the legal system and burden WHRDs with lengthy legal battles.

Anti-terrorism and cybercrime laws, ostensibly created for national security, are frequently manipulated to target WHRDs, limiting their freedom of expression. In India, the Unlawful Activities (Prevention) Act (UAPA) has been systematically used to detain women activists and journalists, creating a chilling effect on their work.[13] In the Philippines, WHRDs are labelled as terrorists under red-tagging policies, facilitated by laws like the Cybercrime Prevention Act and the Anti-Terrorism Act, alongside mechanisms such as the National Task Force to End Local Communist Armed Conflict (NTF-ELCAC) and the Terrorism Financing Prevention and Suppression Act.[14] This pattern is also observed in Ecuador and Brazil, where legal frameworks originally designed to combat crime are instead used to suppress dissent. Tanzania's Cybercrimes Act, 2015 has led to arbitrary arrests of WHRDs, creating a chilling effect on freedom of expression.[15]

In Uganda, obscenity laws have been misused to stifle free speech, with many WHRDs facing criminal charges under vague morality clauses. Interviewees described how these laws have been wielded to target women activists, journalists and LGBTQIA+ rights defenders. The Anti-Homosexuality Act has further exacerbated the situation, not only criminalising LGBTQIA+ individuals but also punishing those who stand in solidarity with them. Several WHRDs reported being harassed, arrested or denied access to legal recourse for supporting LGBTQIA+ rights.

Governments have also imposed stricter regulations on civil society organisations (CSOs), making it increasingly difficult for WHRDs to operate. Many interviewees highlighted financial restrictions as a common form of reprisal, including freezing bank accounts and restricting access to international funds, effectively cutting off financial resources for activists. This practice has been widely reported in the Philippines, India and Uganda, where restrictive policies limit CSOs' ability to receive funding from international organisations.

---

13 Amnesty International and Front Line Defenders. (2024, 24 June). India: Growing concerns on the misuse of Financial Action Task Force standards to target civil society. https://www.amnesty.org/en/wp-content/uploads/2024/06/ASA2082022024ENGLISH.pdf

14 Human Rights Foundation. (2023, 10 April). Red-tagging in the Philippines: A license to kill. https://hrf.org/latest/red-tagging-in-the-philippines-a-license-to-kill/

15 ARTICLE 19. (2020, 31 August). Tanzania: New content regulations criminalise free speech online. https://www.article19.org/resources/tanzania-regulations-criminalise-free-speech/

Unrestrained expansion of surveillance

A growing global surveillance apparatus is systematically targeting WHRDs, fuelled not only by an expanding web of restrictive legislation but also by the widespread deployment of advanced surveillance technologies. Spyware such as Pegasus has been weaponised against defenders in Uganda[16] and Brazil,[17] turning their devices into tools of oppression rather than instruments of resistance. The relentless monitoring of WHRDs, both online and offline, creates a climate of fear, discouraging activism through the ever-present threat of surveillance and retaliation.

Governments do not act alone in this. Their collaboration with private actors has been instrumental in expanding digital surveillance under the guise of security and public order. Laws enabling mass monitoring are often passed with little to no public transparency, reinforcing a culture of secrecy around the deployment of these invasive technologies.

Under the pretext of enhancing public services, biometric data collection for healthcare, national identity programmes and smart city security systems have further encroached upon civic space. Technologies such as facial recognition cameras, AI-driven policing and biometric authentication systems are increasingly deployed to track movements, suppress protests and criminalise activism.

Internet shutdowns and the shrinking civic space

Internet shutdowns have become a strategic weapon against WHRDs, often enforced alongside curfews that further shrink civic space. These digital blackouts are not just disruptions, they are calculated acts of censorship that deepen state and corporate control over information. By severing access to digital platforms, governments and corporations suppress activism, dismantle networks of resistance and erode fundamental rights, fracturing solidarity and revolutionary spaces.

16 Kirabo, J. (2021, 26 November). PEGASUS: Ugandan journalists targeted in spying scandal. *Nile Post.* https://nilepost.co.ug/news/121941/pegasus-ugandan-journalists-targeted-in-spying-scandal

17 Business & Human Rights Centre. (2021, 8 June). Brazil: Million-dollar negotiation for the Pegasus espionage programme, developed by the NSO Group, excluded official government investigation bodies that would directly benefit from the tool. https://www.business-humanrights.org/en/latest-news/brazil-million-dollar-negotiation-for-the-pegasus-espionage-programme-developed-by-the-nso-group-excluded-official-government-investigation-bodies-that-would-directly-benefit-from-the-tool/

In India, for example, the government has used internet shutdowns, increased surveillance and digital censorship to curb protests and control political opposition, particularly in regions such as Kashmir.

In Ecuador, the declaration of a state of emergency with the excuse of combating violence and organised crime, was combined with internet shutdowns, curfews and restricted constitutional rights, including freedom of assembly and protection against warrantless searches. This had a heightened impact on Indigenous rights and on land and environmental defenders.

Digital authoritarianism and extractivism: Control through data and resources

Digital authoritarianism operates hand in hand with a broader culture of extractivism, whether of natural resources through mining and fracking, or of personal data through the non-consensual harvesting of biometrics, geolocation and online activity. Both forms of extraction fuel unchecked accumulation, consolidating power while dispossessing those who resist.

Land defenders and Indigenous WHRDs are at the forefront of this struggle in Brazil, Ecuador and the Philippines, facing violence, displacement and criminalisation for opposing extractive industries. The Big Tech corporations profiting from data extraction are also financially entangled with the industries driving environmental destruction.

Governments and corporations increasingly use big data analytics to track resistance movements and anticipate WHRDs' activism, turning surveillance into a tool of repression. Facial recognition and biometric tracking, justified as tools for territorial mapping and research, are, in reality, instruments of land dispossession and control, disproportionately affecting Indigenous and rural communities.

The criminalisation of defenders is not a new phenomenon, nor is it solely tied to the rise of authoritarian governments. In Latin America, for example, repression escalated alongside the expansion of extractive industries, with mining companies playing a key role in targeting WHRDs. In these regions, organised crime operates with near total impunity, using fear and the absence of accountability mechanisms to evade legal consequences. This entrenched cycle of violence leaves WHRDs increasingly vulnerable, while those responsible for persecution remain invisible within the system.

Privacy and anonymity in the lives of WHRDs

WHRDs describe the stark choices they face when online violence seeps into their everyday lives: either withdraw from their work, communities and homes, or step further into the public eye and fight for the right to exist in those spaces. Both are difficult decisions, each carrying its own risks and consequences.

Many WHRD interviewees spoke of a shift in their activism following threats and violence. The transition from public advocacy to a more discreet, behind-the-scenes role was a recurring theme. For some, stepping away from visibility provided a sense of security, while others struggled with the tension between needing anonymity for safety and the necessity of being heard. One interviewee noted that being forced into the shadows "felt like erasure," while another described the discomfort of relying on invisibility to continue working.

The ability to maintain privacy, as interviewees highlighted, is deeply shaped by context. Those in rural or Indigenous communities often found anonymity impossible. The close-knit nature of these environments meant their personal lives were always under scrutiny, increasing their exposure to stigma, harassment and violence.

For LGBTQIA+ defenders, especially transgender interviewees, visibility itself posed a direct threat. Many recounted experiences of "outing", where their sexual orientation or gender identity was exposed without their consent, leaving them vulnerable to targeted violence. This form of attack was widely reported across the six countries in this study. In Uganda, interviewees spoke of how the Anti-Homosexuality Act had emboldened both state and societal violence, placing

defenders at even greater risk. In Brazil and Ecuador, transgender WHRDs shared harrowing accounts of the extreme violence they faced, from targeted killings to the threat of collective rape as a tool of punishment and control.

For every interviewee, privacy was more than a matter of security, it was also a political struggle, a fight for the right to exist without fear. Yet, as their testimonies reveal, anonymity is rarely a choice freely made; it is a condition forced upon them by the very systems they resist.

IMPACTS

The strengthening of digital authoritarianism reinforces TFGBV against WHRDs by institutionalising surveillance, intimidation and control over information flows. These mechanisms work to force activists into silence, self-censorship or complete withdrawal from digital spaces. Those who remain active online face sustained harassment, reputational harm and threats that frequently extend offline. LGBTQIA+ activists, Indigenous rights defenders, Black, Brown and environmental WHRDs are particularly targeted.

- Silencing and shadow banning: Algorithmic suppression limits the visibility of human rights content online. Coordinated disinformation campaigns distort WHRDs' messages and undermine their credibility. A lack of accountability by tech companies, coupled with the misuse of cybercrime laws, has further restricted freedom of expression and weakened efforts to expose human rights violations.

- Mental health and well-being impacts: WHRDs interviewed reported experiencing chronic stress, burnout, panic attacks, feelings of persecution, hopelessness and collective exhaustion due to ongoing harassment. Some emotionally detach as a coping mechanism, while others internalise the violence as an inevitable cost of their work.

- Distrust in community and networks: Defamation campaigns and the spread of misinformation undermine the legitimacy of WHRDs' work and fracture solidarity networks. Many are forced to relocate or experience social isolation due to threats and violence, perpetrated not only by state agencies and employers, but also within their families. In many cases, law enforcement institutions reinforce violence rather than prevent it.

- Economic impact: Digital violence restricts financial independence. WHRDs who rely on online platforms for their livelihoods, such as journalists, content creators, educators and sex workers, are often forced offline, losing income and in some cases, entire archives of work. The financial burden of SLAPPs and restrictions on funding further jeopardise their sustainability.

- Impunity and normalisation of violence: Online harassment is treated as an expected consequence of activism. Legal protections are weak or non-existent and institutional support is often absent. As a result, WHRDs are left to navigate these threats alone, struggling to continue their work without compromising their safety.

- Undermining of collective action and democratic institutions: The lack of judicial accountability and ongoing delegitimisation of WHRDs has a chilling effect on rights defence, weakening collective action and public trust in democratic systems.

RECOMMENDATIONS

Across the six countries, WHRDs have emphasised the urgent need for holistic digital security strategies grounded in their lived realities. Many underline the importance of accessible, localised and long-term digital safety training. This includes workshops, guidebooks and targeted education on the safe use of social media for community building and advocacy. Funding is another critical concern.

> WHRDs call for resources to be redirected to marginalised communities so that they can create and sustain their own secure digital spaces. This requires investment in gender-sensitive approaches and capacity building, ensuring that digital safety strategies account for the specific risks faced by WHRDs and individuals with marginalised gender identities.

They also point out that most digital protection curricula are rooted in Global North contexts, assuming stable and affordable access to the internet. This disconnect must be addressed. Digital security frameworks need to be relevant, adaptable and inclusive of Majority World realities. Without this shift, digital security remains an exclusive tool rather than a universal right.

The Feminist Holistic Protection framework reminds us that security cannot be reduced to legal protections or individual resilience. It is a collective, intersectional process that must be built from the ground up, centred on the needs, experiences and leadership of WHRDs.

FHP-informed recommendations for strengthening protections against TFGBV:

- Holistic and accessible legal frameworks

Governments should train frontline civil servants, justice sector staff and law enforcement officers to recognise the value of human rights defence and adopt a gender-sensitive approach. This ensures that WHRDs are adequately protected and that institutions respond effectively to threats. Implementing existing protection mechanisms must be a priority.

- Gender-sensitive cybersecurity laws

Legislation should explicitly address digital violence against WHRDs, including doxxing, cyberstalking, online harassment and disinformation campaigns. However, laws alone are insufficient. Without gender-sensitive implementation,

law enforcement authorities may reinforce harm through structural and patriarchal biases. Legal reforms must be paired with holistic training grounded in feminist principles of care, accountability and survivor-centred practice.

- Rapid response mechanisms

Governments and civil society must collaborate to prevent threats from escalating. Coordinated response systems should be in place to provide immediate support when WHRDs are targeted. Emergency mechanisms must offer safe relocation, housing, access to digital safety experts and mental health care. Special attention must be paid to grassroots and rural WHRDs, who often face heightened risks, including state violence.

- Accountability of tech platforms

Companies such as Meta, TikTok, X, Google and others must strengthen their policies and improve content moderation to prevent digital violence and censorship targeting WHRDs. Social media platforms should be required to promptly remove threats, harassment and TFGBV content.

- Legal safeguards against surveillance

Stronger privacy protections must be enforced to prevent mass or arbitrary surveillance under the pretext of national security or public safety. Oversight through judicial review and checks and balances must ensure that surveillance remains proportionate and lawful.

- Uninterrupted internet access

Governments must protect access to the internet by banning shutdowns, throttling and other restrictions that interfere with communication and access to information. Ensuring free and open access to the internet is a foundational requirement for WHRDs' safety and organising.

Country-level recommendations

Through fieldwork, including focus group discussions and interviews, key country-level policy recommendations have been identified. These recommendations require a multi-stakeholder approach, bringing together governments, civil society, digital rights advocates and tech companies to create an ecosystem of protection for WHRDs. By implementing these recommendations, WHRDs can gain holistic access to legal, financial and digital security support, ensuring they can continue their work safely and effectively while combating TFGBV.

Brazil

- Amend Articles 138 to 140 of the Brazilian Penal Code to include explicit safeguards that prevent their use as tools to silence dissent. Without such specific limitations, the laws remain open to arbitrary and strategic misuse.

- The government must hold accountable those responsible for illegal surveillance of WHRDs, activists and journalists, while maintaining transparency in investigative procedures.[18] Representatives of WHRDs must be actively involved throughout the process to ensure that accountability mechanisms reflect the harm caused and do not reproduce further institutional silencing. This includes the reported misuse of technology by ABIN under the previous administration to monitor WHRDs, activists and journalists.[19]

- Strengthen the Brazilian Civil Rights Framework for the Internet (Law No. 12.965/2014) to prevent arbitrary content takedowns, curb mass surveillance, and reinforce protections for WHRDs and activists.

- Mandate stronger content moderation on social media platforms to remove TFGBV-related threats in compliance with Brazil's Marco Civil da Internet.

---

18 During the first three years of the Bolsonaro government, the Brazilian Intelligence Agency (ABIN) operated a secret system for monitoring the location of citizens across the national territory. The tool allowed, without any official protocol, the tracking of the movements of up to 10,000 mobile phone owners every 12 months, through software called "First Mile", developed by the Israeli company Cognyte.

19 Viapiana, T. (2024, 25 January). Brazil's former intelligence chief under investigation for alleged spying on opposition, judges, journalists. *Brazil Reports.* https://www.brazilreports.com/brazils-former-intelligence-chief-under-investigation-for-alleged-spying-on-opposition-judges-journalists/5726/

- Guarantee the implementation of Law 13.642/2018, which addresses the spread of online misogyny, and enforce Law No. 14.532/2023 to combat racial and ethnic hate speech in digital campaigns. This includes protection against digital hate crimes targeting women, LGBTQIA+ individuals and WHRDs.

- Revising the Anti-Terrorism Law (Law No. 13.260/2016) to require stricter judicial review for surveillance requests.

- Ensure the Citizen's Basic Register does not enable mass data collection without oversight.

Ecuador

- Safeguarding WHRDs, journalists and whistleblowers from penalties when exposing corruption, misconduct or threats to public health and safety, ensuring them the right to defend human rights without retaliation.[20] Judicial and prosecutorial training must also be aligned with international human rights standards, so that retaliatory cases are not pursued. In interviews, several WHRDs emphasised the need for independent oversight bodies and fast-response legal support mechanisms to protect those at risk.

- Decriminalise defamation which has been used against WHRDs as a silencing tactic against their activism.

- Reinstate protections against discrimination in media content, by reconsidering the exclusion of Article 61 of the Organic Law of Communications, which explicitly prohibited discrimination based on ethnicity, gender identity, disability and other factors, undermining efforts to counter violence and hate speech in media content.

- Elimination of the "undercover agent" role,[21] which allows agents to access sensitive information without sufficient oversight. Article 77

20 Article 229 of the Penal Code, Article 179 of the Comprehensive Organic Criminal Code.

21 As defined in Article 67 of the Reformative Organic Law to the Strengthening of Institutional Capacities and Comprehensive Security.

establishes the role of an "undercover computer agent" for the purpose of combating cybercrime. This agent is granted broad powers to infiltrate digital spaces, such as preserving and decrypting data, recording images and audio in contact with suspects, and even sending illegal files during investigations. The lack of clear limitations or external oversight over such activities raises serious concerns about violations of privacy, due process, and the potential targeting of WHRDs, journalists, and activists.[22]

- Prevent the use of surveillance as a means of intimidating or harassing WHRDs.[23]

- Implement specific legal provisions to protect WHRDs and organisations from SLAPPs, including sanctions against entities that misuse the legal system to intimidate them. Such provisions could include automatic dismissal of SLAPPs in these contexts and fast-tracking legal aid for those targeted.

- Ensure that the outcomes of environmental consultation processes are legally binding and transparent, requiring that projects cannot proceed without the explicit consent of the affected communities and implementing regular public reporting on the consultation processes and their outcomes.

India

- Strengthen privacy and legal protections by implementing privacy-by-design frameworks, gender-sensitive privacy laws and strict safeguards against state surveillance.

- Prevent misuse of sedition, defamation and anti-terrorism laws (such as UAPA, PMLA and FCRA) to criminalise WHRDs and journalists (including obscenity, hate speech, incitement, etc.) by clarifying vague legal provisions that allow for arbitrary arrests and criminalisation, ensuring due process and fair trial protections, including the right to bail and independent judicial review.

---

22 Sotomayor, A. (2024, 7 August). The Undercover Computer Agent in Ecuador. *Autonomía Digital*. https://autonomia.digital/en/2024/08/07/undercover-digital-agents-in-ecuador.html

23 Revise Article 77 of the Organic Telecommunications Law establishing safeguards for the interception of communications.

- Establish clear legal definitions of TFGBV. Definitions must encompass a range of harms including non-consensual image sharing, cyberstalking, doxxing and digitally enabled threats.

- Ensure streamlined and survivor-centred reporting procedures involving trained, gender-sensitive officials. Authorities must be equipped to act swiftly, such as ordering immediate takedowns of harmful content, without trivialising the violence or introducing harmful delays.

- Access to information procedures must be carried out by state bodies independent from the government so as to ensure that WHRDs have free and safe access to information. While government departments are legally obligated to fulfil such requests, safeguards must be introduced to protect applicants from retaliation, particularly when requests relate to state misconduct. This includes anonymised application options, transparency about how requests are processed, and oversight by independent information commissions or ombudsperson bodies that can intervene when state departments fail to comply or act punitively.

- Bridge algorithmic language gaps by developing Hindi and Hinglish[24] datasets to improve content moderation and digital security. Make phone and platform settings more user-friendly, especially for non-English speakers.

- Prevent arbitrary internet shutdowns by requiring high legal standards and court orders. Establish independent oversight bodies to safeguard WHRDs' access to critical information and protect their right to hold governments accountable.

The Philippines

- Review and amend or repeal problematic surveillance laws, including the National ID System and SIM Card Registration System, which were introduced during Duterte's presidency and have raised serious privacy and security concerns, or any other state surveillance mechanisms that lack judicial oversight, ensuring compliance with human rights standards, judicial review and transparency requirements.

---

24 Hinglish is a hybrid language that blends Hindi and English. It refers to a variety of English shaped by Hindi speakers, where Hindi words, phrases and grammatical structures are frequently woven into English sentences.

- Pass the long-overdue Freedom of Information Act, ensuring the full implementation of the right to access information as provided by the Philippine Constitution and alignment with existing laws, such as the Data Privacy Act, to balance transparency with data protection.

- Strengthen access to information by assigning independent bodies to handle information requests, ensuring transparency and accountability. Years after Duterte's Executive Order No. 2, journalists and civil society groups continue to find it inadequate in fully upholding the constitutional right to access relevant information.

- Repeal the Anti-Terrorism Act (ATA) of 2020, which has been widely used to criminalise HRDs, journalists and activists.

- Reform counterterrorism and counterinsurgency policies to align with human rights standards, including amendments to Countering the Financing of Terrorism (CFT) mechanisms.

- Abolish the National Task Force to End Local Communist Armed Conflict (NTF-ELCAC), as recommended by UN Special Rapporteurs for Freedom of Opinion and Expression and the promotion and protection of human rights.

- Prevent misuse of state resources for political repression.

- Pass the long-pending Human Rights Defenders Protection Law, which cleared the House human rights committee in early 2023. This legislation must safeguard WHRDs and activists from state harassment and violence while ensuring human rights protections take precedence over politically motivated national security claims, preventing the misuse of laws against WHRDs.

- Amend or repeal problematic provisions in the Cybercrime Prevention Act (CPA), including cyber libel, which has been used to silence journalists and WHRDs. As it stands, the provision has been routinely used to harass journalists and human rights defenders through arrest, surveillance and prolonged legal battles. Amendments should also include safeguards to prevent multiple or repeat filings for the same alleged offence, ensure expedited dismissal of SLAPP-type cases and mandate judicial training on freedom of expression and gender-sensitive jurisprudence.

Uganda

- Review surveillance laws, including the Regulation of Interception of Communications Act (2010) and the Computer Misuse Act (2011) to ensure judicial oversight and prevent ambiguity, removing provisions that criminalise online expression and activism.

- Immediately drop all charges and release WHRDs imprisoned for exercising their right to freedom of association and facing charges of incitement or hate speech and revise laws such as the Penal Code Act to decriminalise defamation prevent legal abuse.

- Prevent the use of spyware or digital monitoring tools to target WHRDs, journalists and activists. Ensure that privacy oversight bodies, including the data protection authority and those regulating security forces, operate independently and are adequately resourced to enforce oversight and accountability effectively.

- Align the Access to Information Act with the African Commission's Model Law on Access to Information in Africa (2013) by narrowing exclusions and establishing a clear, effective process for handling information requests.

- Ratify and implement the African Union's Malabo Convention[25] to align national data protection and cybersecurity laws with international human rights standards, ensuring special safeguards for WHRDs, and marginalised groups.

- Immediately repeal the Anti-Homosexuality Act, which violates human rights and fuels discrimination against LGBTQ+ WHRDs, and the Public Order Management Act (2013), which restricts public gatherings and is often used to silence HRDs.

25 The Malabo Convention, also known as the African Union Convention on Cyber Security and Personal Data Protection, is a regional treaty adopted by the African Union in 2014. It aims to establish a regulatory framework for cybersecurity, data protection and electronic transactions and to combat cybercrime across African countries.

- Undertake a review of taxation and other provisions affecting the cost of access to the internet with gender mainstreaming treated as a priority with regard to the state's ICT and tax policies and prevent politically motivated shutdowns, as seen during elections and protests.

- Reform the Non-Governmental Organisations Act 2016 to align with international human rights standards, removing restrictions on NGO registration and ensuring an independent oversight mechanism for reviewing registration decisions.

- Eliminate barriers preventing WHRDs and NGOs from receiving donor funding essential to their work.

Tanzania

- Review the Cybercrimes Act (2015) to remove vague provisions that allow for arbitrary surveillance and criminalisation of online expression and to include protections against TFGBV.

- Revise the Electronic and Postal Communications Regulations (2020) to remove restrictions on online speech, including the $900 registration fee for bloggers and content creators. Amend the Media Services Act (2016) to eliminate restrictive accreditation requirements for journalists, safeguarding press freedom.

- Ratify and enforce the African Union's Malabo Convention, ensuring national data protection and cybersecurity laws align with international human rights standards and include explicit safeguards for WHRDs and marginalised communities against digital threats and state surveillance.

- Align the Access to Information Act (2016) with the African Commission's Model Law on Access to Information (2013).

- Ensure the Prevention of Terrorism Act (2002) is not weaponised to suppress dissent or target WHRDs.

- Amend the Statistics Act (2015) to guarantee independent researchers and journalists the right to publish without government approval.

- Amend the NGO Act (2002) and related regulations to eliminate barriers to civil society, ensuring WHRDs and NGOs can register and operate free from government interference.