The Commonwealth

Commonwealth Cyber Journal \ 119
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

Cyberstalking and Technology-Facilitated Intimate Partner Violence: A Review of Three African Countries

Chioma Andeh

Abstract

Cyberstalking and technology-facilitated intimate partner violence (TFIPV) have emerged as critical challenges in the digital age, allowing abusers to monitor, exert control over and intimidate victims beyond physical spaces. With the widespread adoption of smartphones, social media and GPS tracking, digital tools are increasingly weaponised in intimate relationships, exacerbating psychological, emotional and physical harm.

This study examines the impact of TFIPV in three countries in Africa – Kenya, Nigeria and South Africa – that have enacted legislative measures to regulate technology companies and address digital abuse. Given the limited scope of relevant legal frameworks across the continent, additional cases are considered to provide a broader comparative perspective. The study explores prevalent cyberstalking tactics, including spyware deployment, unauthorised access to personal data, location tracking and social media harassment. It further analyses the gendered dimensions of these abuses, highlighting the heightened vulnerabilities of marginalised groups, including women with limited literacy, those in rural areas and women with disabilities.

In addition to assessing African legal responses, this study reviews global initiatives to combat cyberstalking and TFIPV, analysing international legal frameworks, policy interventions and corporate accountability measures. By comparing regional and global approaches, the study identifies best practices and enforcement gaps that hinder victim protection and legal redress.

The findings underscore the urgent need for stronger legal frameworks, enhanced digital literacy programmes and increased accountability from technology companies. The study concludes with policy recommendations and technological innovations aimed at mitigating digital abuse, protecting survivors and fostering safer online environments.

1. Introduction

1.1 Background, definitions and theoretical framework

The rapid proliferation of digital technology has redefined human communication and interpersonal relationships, offering both transformative opportunities and unprecedented risks. While digital tools enhance connectivity and democratise access to information, they also create new avenues for harm, particularly in cases of intimate partner violence (IPV). The World Health Organization (WHO, 2021) defines IPV as the infliction of physical, sexual, psychological or emotional harm by a current or former partner. Cyberstalking, a digital extension of traditional stalking, involves persistent online surveillance, harassment and intimidation through platforms such as social media, smartphones and GPS tracking (Reed et al., 2022).

A robust theoretical framework is essential for understanding these phenomena. Feminist technology theory (Wajcman, 2004) examines how digital innovations can both challenge and reinforce gendered power structures, highlighting the paradox in which technology, designed to empower, may also facilitate coercive control. Complementing this perspective, power and control theories (Pence and Paymar, 1993) explore how abusers leverage digital tools to extend coercive control, further restricting victims' autonomy and agency.

1.2 Psychological underpinnings of digital abuse

Psychological theories offer further insights into the motivations behind technology-facilitated IPV (TFIPV) and its effects on victims. Attachment theory (Bowlby, 1969) suggests that individuals with insecure attachment styles may resort to obsessive surveillance and control behaviours as maladaptive mechanisms to maintain relational dominance. Meanwhile, the online disinhibition effect (Suler, 2004) explains how digital anonymity and reduced accountability embolden perpetrators to engage in harassment and stalking – behaviours they might avoid in face-to-face interactions.

These dynamics contribute to learned helplessness (Seligman, 1975), where victims feel trapped because of the pervasive nature of digital abuse. Continuous monitoring, digital manipulation and online threats erode victims' sense of agency, exacerbating psychological trauma and increasing dependency on their abusers.

1.3 Power dynamics in technology-mediated relationships

Technology has restructured power dynamics in intimate relationships, particularly in abusive contexts. Digital tools offer perpetrators multiple avenues for coercive control, extending their influence beyond physical presence. Some of the key strategies include:

- **Surveillance and monitoring**: Perpetrators use spyware, GPS tracking and social media monitoring to track victims' activities, reinforcing dominance and restricting autonomy (Douglas et al., 2019).
- **Digital harassment and social manipulation:** Abusers engage in online shaming, impersonation and misinformation campaigns to isolate victims and undermine their credibility. Doxing, or the public exposure of private information, has become an increasingly common tool to instil fear and compliance (Rege, 2020).
- **Economic control via technology:** Financial abuse in TFIPV includes monitoring mobile banking apps, restricting access to online employment opportunities and weaponizing digital financial services to create financial dependency (Woodlock, 2017).

While technology can be a tool for oppression, it also has the potential to empower IPV survivors. Digital platforms provide avenues for accessing support networks, reporting abuse and seeking legal assistance. However, without proper safeguards, these same platforms can be weaponised against victims, highlighting the dual role of technology in IPV contexts.

1.4 Focus on Africa: relevance and scope

Africa presents a unique and compelling context for examining TFIPV, given the rapid digital transformation occurring alongside systemic socio-economic and legal challenges. While mobile and internet penetration have increased significantly, many African countries lack adequate regulatory frameworks for digital safety and cybercrime enforcement. Weak legal infrastructure, combined with socio-cultural barriers such as stigma, economic dependency and patriarchal dominance, exacerbates the risks IPV survivors face.

Studies indicate that in Nigeria, over 60 per cent of IPV cases involve a digital component, yet fewer than 20 per cent of survivors report abuse, out of fear of social backlash and distrust in legal institutions (Aderibigbe, 2021). Similarly, Kenya has witnessed a sharp rise in cyber-related IPV, particularly among women, as perpetrators exploit social media and location-tracking tools (Mwangi and Otieno, 2021). In South Africa, where the internet penetration rate is among the highest on the continent, digital stalking and online harassment are escalating threats, yet law enforcement mechanisms remain weak and inconsistent (Chigbu et al., 2020a).

2. Methodology and literature review

This section outlines the research design, data collection methods and analysis approach while situating the study within the broader academic discourse on cyberstalking and TFIPV. The research focuses on Kenya, Nigeria and South Africa, where digital technology has transformed intimate relationships, introducing new forms of control, surveillance and coercion in IPV.

2.1 Research design and data collection

Given the complex and evolving nature of TFIPV, a qualitative research design was adopted. This approach is well suited to capturing the socio-legal dimensions and psychosocial effects of digital abuse in intimate relationships. The study employs a systematic scoping review of academic literature, policy reports, legal frameworks and case studies from the selected countries.

Scoping review approach

A systematic review of peer-reviewed journal articles, legal statutes and organisational reports was conducted using JSTOR, SpringerLink, SAGE Journals and Google Scholar. Search parameters were restricted to studies published between 2015 and 2025 to ensure relevance.

The research aimed to:

- Analyse the prevalence, forms and impact of TFIPV in Kenya, Nigeria and South Africa;
- Examine the role of digital technology in facilitating IPV;
- Evaluate the effectiveness of legal responses and institutional mechanisms in addressing TFIPV.

Search strategy and selection criteria

The literature search incorporated thematic keywords such as 'cyberstalking', 'technology-facilitated intimate partner violence', '' 'Kenya', 'Nigeria', 'South Africa' and 'cyber harassment'.

Studies were included if they:

- Focused on cyberstalking or TFIPV in Kenya, Nigeria or South Africa;
- Were empirical research studies, systematic reviews or policy analyses;
- Provided legal, psychological or socio-cultural insights on TFIPV.

Studies were excluded if they lacked empirical or theoretical grounding or were purely opinion-based without substantive evidence.

Data extraction and thematic analysis

A structured data extraction framework was developed to classify sources based on:

- Study objectives and methodologies;
- Findings on prevalence and impact;
- Legal and policy implications.

A thematic analysis was conducted, identifying emerging patterns related to:

- Surveillance and coercive control mechanisms in IPV;
- Legal and institutional gaps in addressing TFIPV;
- Socio-cultural factors influencing digital abuse.

Ethical considerations

Although this study relies on secondary data, ethical integrity was maintained by:

- Ensuring accurate attribution of sources (Douglas et al., 2019; Rege, 2020);
- Documenting selection criteria and methodology for transparency;
- Critically appraising sources to minimise bias.

2.2 Literature review

The literature on cyberstalking as an extension of IPV has expanded significantly in recent years. This section examines key themes in the existing literature, including the role of technology in enabling abuse, legal and policy challenges, and regional responses.

2.2.1 Cyberstalking in the context of intimate partner violence

The widespread use of social media, smartphones and location-tracking tools has reshaped intimate relationships, making cyberstalking a dominant form of coercive control in IPV cases (Douglas et al., 2019; Rege, 2020). Victims often experience persistent surveillance, online harassment and unauthorised access to personal information.

Studies indicate that cultural interpretations of digital control further complicate victim responses. In Nigeria, some victims misinterpret persistent online surveillance as an expression of affection, reinforcing coercive behaviours within intimate relationships

(Aderibigbe, 2021). In South Africa, victims report heightened levels of psychological distress resulting from the continuous presence of abusers in their digital spaces (Nkosi, 2022).

2.2.2 The role of technology in enabling abuse

Digital tools such as social media, spyware and tracking applications have revolutionised how abusers perpetrate IPV. These technologies facilitate a seamless transition of abuse from the offline to the online environment, thereby increasing isolation, fear and dependency among victims (Dragiewicz et al., 2019). In Africa, economic disparities and variations in digital literacy compound these challenges. Rural victims, in particular, may lack the skills to recognise or counteract digital surveillance; urban victims may face overwhelmed support services and insufficient legal protections (Chigbu et al., 2020b).

2.2.3 Country-specific legal frameworks and enforcement challenges

A country-specific analysis of TFIPV prevalence, legal protections and enforcement gaps in Kenya, Nigeria and South Africa provides insights into the effectiveness and limitations of existing laws. While these nations have established cybercrime laws, challenges persist in legal enforcement, digital forensic capacity and victim support mechanisms.

Kenya

Prevalence and manifestations

Kenya has experienced a rise in cyber-related IPV, particularly affecting women and LGBTQ+ individuals. Studies estimate that 30–35 per cent of internet users have been victims of online stalking, digital impersonation or image-based abuse (Kamau and Njoroge, 2021). Perpetrators often exploit social media and location-tracking technologies to harass, threaten or blackmail victims (Mutua, 2019).

Legal framework

Kenya has introduced laws targeting cybercrime, but gaps remain in IPV-specific digital protections:

- The Computer Misuse and Cybercrimes Act (2018) prohibits cyber harassment and unauthorised monitoring but does not address scenarios where victims are coerced into sharing access credentials.
- The Kenya Data Protection Act provides data privacy protections but lacks provisions safeguarding IPV survivors from tech-facilitated surveillance.

Enforcement challenges

Several barriers impede the effectiveness of legal measures:

- **Limited technical capacity:** Law enforcement lacks adequate cyber forensic training, leading to low prosecution rates (Njogu, 2020).
- **Lack of victim-centred protections:** Most laws do not consider power imbalances in intimate relationships, allowing abusers to manipulate legal loopholes (Mutua, 2019).
- **Overburdened legal system:** Kenya's judiciary faces case backlogs, delaying justice for IPV survivors (KICTANet, 2022).

Nigeria

Prevalence and manifestations

Nigeria has witnessed a significant increase in cyberstalking, online harassment and digital surveillance as tools of IPV. Estimates suggest that 30–35 per cent of Nigerian internet users have experienced cyber harassment, GPS tracking or unauthorised digital surveillance (Okafor, 2020; Adebayo and Musa, 2021).

Legal framework

Nigeria has enacted several laws to address cyberstalking and online harassment, yet gaps remain in protecting IPV survivors:

- The Cybercrimes (Prohibition, Prevention, Etc.) Act (2015) criminalises cyberstalking and electronic harassment but does not adequately account for intimate partner contexts, where abusers may have pre-existing access to victims' digital lives.
- The Nigeria Data Protection Regulation 2019 aims to safeguard personal data but lacks explicit provisions addressing coercive control through digital access in IPV settings (Mba et al., 2020).

Enforcement challenges

Despite the legal provisions, several systemic barriers hinder enforcement:

- **Limited digital forensic capacity:** Law enforcement agencies lack expertise in gathering digital evidence, leading to low conviction rates (Adeyemi, 2018).
- **Cultural misconceptions:** Some victims misinterpret digital surveillance as an expression of care, reinforcing coercive control dynamics (Eze and Chukwudi, 2019).
- **Lack of institutional co-ordination:** Poor collaboration between law enforcement, judicial bodies and digital platforms weakens victim protection mechanisms (Hinson et al., 2018).

South Africa

Prevalence and manifestations

South Africa has among the highest rates of both offline and online IPV in Africa. Studies indicate that one-third of South Africans report cyberstalking, non-consensual image distribution or digital harassment (Smith et al., 2019). Digital abuse is particularly prevalent among women in urban areas, where high internet penetration increases exposure to tech-facilitated abuse (Moyo and Nkosi, 2020).

Legal framework

South Africa has a more developed cybercrime legal framework, yet enforcement remains inconsistent:

- The Protection from Harassment Act 2011 recognises cyber harassment as a legal offense but does not explicitly cover TFIPV.
- The Cybercrimes Act (2020) criminalises revenge pornography, cyberstalking and unauthorised access to digital information; however, enforcement is often hampered by lack of technical expertise (Nkosi, 2022).

Enforcement challenges

Despite strong legal provisions, enforcement remains weak owing to structural constraints:

- **Underreporting owing to stigma:** Victims often avoid legal action out of fear of retaliation or social judgement, particularly in patriarchal communities (Department of Home Affairs, 2021).
- **Judicial delays:** Backlogs in cybercrime cases lead to prolonged legal processes, discouraging victims from seeking justice (Watson et al., 2022).
- **Resource constraints:** Insufficient training of law enforcement officials in handling digital evidence collection and lack of adequate cyber forensic training, leading to low prosecution rates (Njogu, 2020).

2.2.4 Broader challenges in legal frameworks

Despite legislative advancements in Kenya, Nigeria and South Africa, several cross-cutting legal challenges undermine the effectiveness of legal protections against TFIPV across African jurisdictions. These challenges include:

- Lack of IPV-specific digital protections: Most cybercrime laws criminalise cyberstalking but fail to account for coercive control within intimate relationships (Nkosi, 2022). Existing laws often treat digital abuse as isolated incidents rather than part of a broader pattern of IPV.

- Weak law enforcement training in digital forensics: Many African law enforcement agencies lack cyber forensic expertise, making it difficult to gather digital evidence and prosecute cases effectively (Aderibigbe, 2021). Without specialised training, officers may dismiss cyberstalking complaints or fail to trace online perpetrators.
- Jurisdictional limitations and cross-border cybercrime: Perpetrators often use social media, virtual private networks or offshore digital platforms to evade law enforcement. Since many African cybercrime laws are restricted to domestic jurisdiction, authorities struggle to hold online abusers accountable when attacks originate from outside national borders (Watson et al., 2022).
- Limited collaboration between governments and technology companies: While global tech firms (e.g., Meta, Google) have introduced reporting tools and privacy features, there is little direct collaboration between African governments and social media companies to proactively curb digital abuse (Mason, 2021). Many victims report that their abuse reports on social media are ignored or inadequately addressed.
- Inconsistent implementation of cybercrime laws: While several African countries have enacted cybercrime legislation, their enforcement is often weak, inconsistent or hindered by judicial delays (Chigbu et al., 2020b). In many cases, victims report that police trivialise digital abuse complaints, advising survivors to simply block the perpetrator instead of launching investigations (Mwangi and Otieno, 2021).
- Cultural barriers and victim stigmatisation: Social norms often discourage victims from reporting digital abuse, especially in rural and patriarchal communities. Victims may be blamed for engaging in online spaces or told that cyberstalking is a private matter rather than a criminal offence (Eze and Chukwudi, 2019).

2.2.5 Comparative insights from Morocco, Rwanda and Uganda

While the primary focus of this study is on Nigeria, South Africa, and Kenya, examining the legal frameworks in Morocco, Rwanda and Uganda provides valuable regional context. Morocco has made strides with a new criminal code targeting cyber blackmail and sexual harassment; however, the application of this to TFIPV remains limited by cultural stigmas and enforcement challenges (Zouiten, 2024). In Rwanda, despite the explicit criminalisation of cyberstalking, the penalties do not always serve as effective deterrents, particularly in cases of IPV where the abuse is intertwined with personal relationships. In Uganda, existing laws such as the Anti-Pornography Act, although intended to curb digital abuse, often criminalise survivors of TFIPV as a result of overlapping provisions and societal prejudices (Nyeko, 2023).

2.3 Synthesis and research implications

The country-specific analysis underscores systemic weaknesses in addressing TFIPV, revealing key gaps in legislation, enforcement and victim support.

- Legal frameworks exist but lack IPV-specific protections. Laws generally criminalise cyberstalking and harassment but fail to recognise the nuanced power dynamics in intimate relationships (Nkosi, 2022).
- Weak enforcement undermines legislative progress. Many cases go unreported or unprosecuted as a result of limited technical training and case backlog issues (Aderibigbe, 2021).
- Cultural and economic factors hinder victim protection. Stigma, financial dependency and digital illiteracy prevent many survivors from seeking help (Chigbu et al., 2020a).

3. Mechanisms of cyberstalking in intimate partner violence

The integration of technology into IPV has significantly altered the ways in which abuse is perpetrated. Cyberstalking enables abusers to exert control, monitor and harass their victims remotely, leveraging digital tools such as social media, GPS tracking, spyware and online threats. These mechanisms disproportionately impact women, particularly those from marginalised communities, whose vulnerabilities are exacerbated by cultural norms, economic dependency and systemic inequities. This section explores the key mechanisms of cyberstalking within IPV and examines how gendered vulnerabilities shape the experiences of victims in African contexts.

3.1 Mechanisms of cyberstalking in intimate partner violence

Cyberstalking within IPV manifests through multiple digital tactics, each reinforcing the abuser's control over the victim.

3.1.1 Social media surveillance

Social media platforms such as Facebook, Instagram and WhatsApp provide abusers with extensive opportunities to monitor victims' activities, interactions and locations.

- **Tactics of surveillance:** Abusers create fake profiles to track victims, impersonate them to manipulate relationships and spread misinformation, or demand access to victims' accounts through coercion.

- **Psychological impact:** Victims engage in self-censorship, restricting online interactions out of fear of retaliation. The constant surveillance erodes privacy and autonomy, reinforcing entrapment. Studies in Kenya indicate that social media surveillance contributes to social isolation and emotional exhaustion among victims (Mwangi and Otieno, 2021).

3.1.2 GPS and location tracking

The widespread availability of GPS-enabled devices has provided abusers with advanced tools to track victims' movements in real-time.

- **Methods:** Abusers use applications such as Find My iPhone or Life360 to secretly track victims. GPS trackers placed on vehicles or personal belongings allow them to monitor movements without consent.
- **Consequences:** Victims report feeling constantly monitored, fearing retaliation if they deviate from expected routines. In South Africa, a case study revealed that a woman's partner had secretly tracked her for months, leading to increased psychological distress and further isolation (Nkosi, 2022).

3.1.3 Spyware and unauthorised access

Spyware applications enable abusers to infiltrate victims' digital devices, gaining unauthorised access to private communications and online activities.

- **Common tools**: Spyware such as FlexiSPY and mSpy allows abusers to monitor text messages, emails and call logs in real time. Many victims unknowingly have such software installed on their devices or are coerced into revealing their passwords.
- **Impact on victims**: The invasive nature of spyware fosters constant fear and helplessness, making it difficult for victims to escape abusive relationships. In Nigeria, spyware use has been identified as a significant barrier for women attempting to seek help or leave abusive partners (Aderibigbe, 2021).

3.1.4 Digital harassment and threats

Cyberstalking often extends beyond monitoring to direct digital harassment, including threats, blackmail and non-consensual sharing of intimate images.

- **Forms of harassment**: Abusers send threats through email or social media, often coercing victims into compliance. Revenge pornography, where abusers share or threaten to share explicit images, is a particularly harmful tactic used to humiliate and control victims.

- **Barriers to protection:** Despite the criminalisation of digital harassment in some African countries, victims face difficulties in proving abuse because of the challenges of collecting evidence. Additionally, many are deterred by societal stigma and fear of retaliation (Chigbu et al., 2020b).

3.2 Gendered vulnerabilities and systemic barriers

Women, particularly those from marginalised communities, face heightened risks of cyberstalking and TFIPV as a result of entrenched structural inequalities, cultural expectations and economic dependency.

3.2.1 Disproportionate impact on women

Research suggests that over 60 per cent of women in IPV situations in Africa have experienced cyberstalking, with social media surveillance and GPS tracking being the most commonly reported methods of abuse. The psychological toll includes heightened anxiety, fear and symptoms of post-traumatic stress disorder (PTSD), as digital monitoring creates an omnipresent sense of surveillance and entrapment (Nkosi, 2022). Societal norms further reinforce victim-blaming attitudes, discouraging women from seeking legal or social recourse (Aderibigbe, 2021).

3.2.2 Unique vulnerabilities of marginalised women

Certain groups of women face compounded risks linked to social, economic and systemic factors:

- **Women with disabilities:** Abusers exploit their reliance on technology for communication and healthcare, using digital tools to isolate and manipulate them. Limited access to legal and social services further exacerbates their vulnerability (Chigbu et al., 2020a).
- **Women from lower socio-economic backgrounds:** Financial dependence makes it difficult for these women to leave abusive relationships. Many lack digital literacy, leaving them unaware of how to protect themselves from spyware or tracking apps. Rural women are particularly at risk as a consequence of restricted access to education and digital resources (Mwangi and Otieno, 2021).
- **Women from marginalised ethnic groups:** Cultural biases and systemic discrimination often prevent these women from reporting abuse. In Nigeria, for example, expectations of familial loyalty deter victims from seeking help, reinforcing cycles of digital and physical IPV (Aderibigbe, 2021).

3.2.3 Cultural and social norms exacerbating risk

- **Cultural silence and victim-blaming:** In many African societies, IPV is normalised, and victims are discouraged from speaking out to preserve family harmony. Fear of retaliation or social backlash often forces women to endure abuse in silence (Nkosi, 2022).
- **Technological literacy and access:** Many women, particularly in rural and underserved communities, lack awareness of digital security tools that could protect them from cyberstalking. Without knowledge of privacy settings, secure passwords or protective applications, victims remain highly vulnerable to invasive technologies (Mwangi and Otieno, 2021).

3.3 Economic and structural barriers to protection

Financial dependency, inadequate legal enforcement and lack of institutional support further entrench victims in digitally abusive relationships.

- **Economic barriers:** Many victims are financially reliant on their abusers, limiting their ability to access secure devices, legal assistance or digital safety training. In Nigeria, economic constraints are a significant factor preventing women from escaping abusive relationships (Aderibigbe, 2021).
- **Weak legal protections and enforcement:** While some African nations have criminalised digital harassment, enforcement remains inconsistent owing to a lack of specialised training among law enforcement personnel. Victims frequently report that authorities dismiss their claims or lack the technical skills to collect digital evidence effectively (Chigbu et al., 2020a).
- **Limited collaboration with technology companies:** Although social media platforms have introduced safety features, their effectiveness in IPV cases is limited. Reporting mechanisms are often slow, and technology firms lack streamlined processes for assisting law enforcement in cyberstalking cases (Mason, 2021).

4. The impact of cyberstalking and law enforcement negligence in addressing TFIPV

The psychological toll of cyberstalking in IPV is profound, often surpassing that of traditional forms of abuse. Unlike physical violence, which leaves visible marks, digital abuse is persistent, invasive and difficult to escape. Cyberstalking intensifies emotional trauma, induces feelings of helplessness and isolates victims in ways that significantly hinder their ability to seek help. Additionally, barriers to reporting and inadequate law enforcement responses exacerbate the harm experienced by victims, leaving them vulnerable to ongoing abuse.

4.1 Psychological and emotional effects of cyberstalking

Cyberstalking imposes severe psychological consequences, including anxiety, depression and PTSD. Victims often experience chronic anxiety from knowing their every move may be monitored, creating a persistent state of fear that undermines their mental health and sense of security (Cowan and Boyle, 2019). The emotional toll frequently results in depression and PTSD symptoms such as nightmares, flashbacks and hyperarousal (Priebe et al., 2017). The psychological distress is heightened when abusers exploit GPS tracking, spyware or hidden cameras to exert control over victims, making them feel powerless and constantly watched (Baker and Stonard, 2021).

4.2 Feelings of helplessness and entrapment

Cyberstalking fosters a profound sense of entrapment for victims. The continuous surveillance, digital harassment and online threats often make victims feel unable to escape abusive relationships. Abusers exploit victims' dependence on technology to control them, monitoring messages, dictating social interactions and restricting access to online platforms (Baker and Stonard, 2021). Victims frequently report losing autonomy, experiencing deepening isolation and becoming increasingly dependent on their abusers. This digital control tends to escalate over time, reinforcing the cycle of abuse. Many victims hesitate to leave their homes or maintain personal connections owing to fear of retaliation or intensified abuse.

4.3 Social isolation and economic control

Cyberstalking and digital abuse exacerbate social isolation by severing victims' connections to their support networks. Abusers may force victims to block contacts, delete social media accounts or stop communicating with friends, further increasing their psychological dependence (Watson and Joubert, 2022). Economic dependence also heightens vulnerability, particularly when abusers manipulate digital tools to control finances – denying victims access to accounts, restricting online banking or interfering with professional communication (Nkosi, 2022). The lack of financial independence makes it even harder for victims to escape abusive relationships.

4.4 Barriers to seeking help and documenting abuse

Despite the severity of cyberstalking in IPV, significant barriers prevent victims from seeking legal protection:

- **Difficulties in documenting digital abuse:** Many victims lack the technical expertise to track spyware, recover deleted messages or gather digital evidence. This makes it challenging to prove harassment to law enforcement or in court (Aderibigbe, 2021).

- **Law enforcement's limited technical knowledge:** Police officers often lack training in cybercrime investigation and struggle to handle digital evidence effectively (UNODC, 2011).
- **Victim-blaming and dismissive attitudes:** Victims frequently report being dismissed, ridiculed or advised to 'just block the perpetrator' rather than receiving meaningful legal support (Mwangi and Otieno, 2021).
- **Fear of retaliation:** Many survivors hesitate to report cyberstalking out of fear that abusers will escalate their threats or retaliate, particularly when perpetrators have access to victims' digital devices (Aderibigbe, 2021).

4.5 Law enforcement failures in addressing TFIPV

Despite the rising prevalence of TFIPV, law enforcement in many African countries has struggled to investigate and prosecute cases effectively. Key challenges include outdated legal frameworks, lack of digital forensic capabilities and systemic neglect.

4.5.1 Case studies: law enforcement negligence

Several high-profile cases illustrate law enforcement's failure to address TFIPV effectively:

- **Kenya – the murder of Ivy Wangechi (2019):** Ivy Wangechi, a 26-year-old university student, was murdered by her stalker after months of online harassment and threats. Despite filing complaints, law enforcement failed to intervene, ultimately leading to her tragic death (Musambi and Inganga, 2024).
- **Nigeria – international sextortion case (2024):** A Nigerian man was extradited to the US after operating a sextortion scheme that led to the suicide of a South Carolina teenager. This case exposed gaps in Nigeria's cybercrime enforcement, as similar domestic cases often remain underreported and uninvestigated (Collins, 2024).
- **South Africa – dismissal of cyber harassment complaints (2022):** A South African woman reported persistent digital stalking, but police dismissed her complaint and advised her to 'just block the number' instead of offering legal recourse (UNODC, 2011).

4.5.2 Notable incidents of cyberstalking and digital harassment in Africa

- **Kenya – cyberattacks and digital violence (2024):** Hackers targeted government platforms, exposing cybersecurity vulnerabilities. Victims of cyber harassment struggled to obtain police assistance owing to wider instability in Kenya's digital security systems (Jackson, 2024).

- **Nigeria – social media scams and online harassment (2024):** Meta removed over 63,000 fake Nigerian Instagram and Facebook accounts linked to romance scams, identity theft and cyber harassment. Despite victims' reports, law enforcement follow-up remained inadequate (Adeoye, 2024).
- **South Africa – digital stalking and revenge pornography:** Despite legal protections under the Cybercrimes Act, many cases of cyberstalking and revenge pornography remain unresolved owing to weak enforcement and limited police resources (Ekanem, 2024).
- **Africa-wide sextortion networks:** Reports reveal that sextortion networks across Africa have blackmailed thousands of victims, yet law enforcement fails to provide consistent legal protection (Ekanem, 2024).

5. Combating cyberstalking in TFIPV

Cyberstalking, as a form of TFIPV, requires a comprehensive, evidence-based and policy-driven approach to effectively combat it. This includes legal reforms, digital literacy initiatives, enhanced victim support, industry accountability and international co-operation. However, moving beyond broad recommendations, it is crucial to outline concrete, actionable steps for implementation, ensuring technological, legal and institutional mechanisms work together to protect victims.

This section examines ongoing global and regional initiatives to combat TFIPV while presenting key recommendations for legal enforcement, victim assistance, digital security measures and international co-operation.

5.1 Ongoing global and regional efforts to combat TFIPV

Several international and regional initiatives have been developed to address cyberstalking within IPV. These efforts focus on harmonising legal frameworks, fostering cross-sector collaboration and leveraging technology for prevention and intervention.

5.1.1 Global initiatives

Budapest Convention on Cybercrime

The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention (2001), provides an international legal framework to combat cybercrime, including cyberstalking. Adopted in 2001, the Convention facilitates the harmonisation of national laws, promotes international co-operation and establishes procedures for investigating and prosecuting cybercrimes. It is considered the benchmark for developing global legal standards to address technology-facilitated abuse.

WePROTECT Global Alliance

The WePROTECT Global Alliance is a multi-stakeholder initiative that unites governments, technology companies and civil society organisations to combat online abuse and exploitation. Its focus extends to TFIPV, as it promotes evidence-based policies and practices to safeguard vulnerable groups. The alliance's Global Threat Assessment Report highlights emerging threats and provides recommendations for addressing technology-facilitated violence (WePROTECT Global Alliance, 2022).

Making All Spaces Safe Programme (UNFPA)

The Making All Spaces Safe Programme, under the United Nations Population Fund (UNFPA), specifically addresses technology-facilitated gender-based violence. The initiative aims to fill critical gaps in prevention and response by integrating targeted activities into existing gender-based violence programming. It promotes rights-based laws and safety-by-design standards in technology development. With pilot programmes in Benin and Kenya, the initiative employs a participatory, context-driven approach to ensure tailored and sustainable solutions for communities (UNFPA, 2022).

Digital Services Act (EU)

The Digital Services Act enacted by the EU establishes robust regulations for online platforms, mandating them to proactively combat online harassment and abuse. The Act holds technology companies accountable for ensuring user safety, requiring transparency in content moderation and the implementation of effective reporting mechanisms.

Global Network Initiative

The Global Network Initiative brings together technology companies, academics and human rights organisations to promote privacy and freedom of expression online. It provides a framework for companies to address online harassment while safeguarding digital rights, emphasising the importance of transparency and accountability in mitigating cyberstalking and TFIPV (GNI, 2021).

Girls Can Code Initiative (ITU)

The International Telecommunication Union (ITU) Girls Can Code Initiative is an educational programme aimed at equipping women and girls with technical skills to safely navigate digital spaces. By enhancing digital literacy, the initiative empowers women to recognise, prevent and respond to online abuse, fostering resilience against technology-facilitated violence (ITU, 2022).

5.1.2 African-focused efforts

Efforts to combat TFIPV in Africa span regional, national and grassroots levels. These initiatives focus on legal reforms, policy harmonisation, victim protection and digital literacy programmes to create safer online environments and empower survivors of digital abuse.

Convention on Cyber Security and Personal Data Protection (AU)

Known as the Malabo Convention, the Convention on Cyber Security and Personal Data Protection, adopted by the AU in 2014, serves as a foundational regional instrument in combating cybercrime, including cyberstalking and digital abuse. It urges member states to criminalise technology-facilitated abuse, establish robust frameworks for victim protection and harmonise cybercrime laws across African nations. By advocating for uniform legal responses and cross-border co-operation, the Malabo Convention seeks to strengthen regional cybersecurity governance. However, its adoption and implementation remain inconsistent, with many African nations yet to ratify or fully integrate its provisions into domestic law (Bakibinga, 2022).

National legislative efforts on TFIPV

Several African countries have enacted legal frameworks to address TFIPV, including Kenya, Morocco, Nigeria, Rwanda, South Africa and Uganda. Laws such as the Computer Misuse and Cybercrimes Act (Kenya 2018), the Cybercrimes (Prohibition, Prevention, Etc.) Act (Nigeria 2015) and the Cybercrimes Act (South Africa 2020) criminalise cyberstalking, online harassment and unauthorised access to digital information. Additionally, Morocco's Law No. 103-13 2018 on Combating Violence Against Women, Rwanda's Cybercrime Law 2020 and Uganda's Computer Misuse Act 2011 contain provisions addressing online abuse. While these legislative efforts demonstrate progress, enforcement gaps, limited law enforcement capacity and low public awareness continue to hinder their effectiveness (Moyo and Nkosi, 2020). Greater focus on implementation and survivor-centred legal responses is essential to strengthening protections against digital IPV.

Paradigm Initiative and Digital Rights Advocacy

The Paradigm Initiative (PIN) is a leading digital rights advocacy organisation in Africa, working to ensure cybercrime laws incorporate protections for IPV survivors. Through research, policy engagement and legal aid, PIN provides critical support for victims of digital abuse while pushing for survivor-centred legislation. The organisation also offers digital security training, equipping women with the knowledge to protect themselves from online threats. PIN's advocacy efforts have contributed to key policy discussions on cyber rights and safety, influencing legal reforms in multiple African countries (PIN, nd).

FEMNET and policy reform for women's digital safety

FEMNET, a pan-African feminist network, actively engages governments and regional bodies to promote policies that protect women from online harassment and digital violence. The organisation works on gender and technology issues, advocating for stronger legal frameworks that address TFIPV. FEMNET also collaborates with civil society groups to raise awareness of digital gender-based violence and supports initiatives that provide legal aid to survivors. By integrating feminist perspectives into policy discussions, FEMNET ensures legal and technological interventions remain gender-sensitive and survivor-centred (FEMNET, nd).

Safe Sisters programme and digital security training

The Safe Sisters programme is a grassroots initiative aimed at equipping women with practical cybersecurity skills to protect themselves from online abuse. Through workshops and mentorship, it empowers survivors with knowledge on securing personal data, recognising digital threats and implementing protective measures against cyberstalking and digital harassment. The programme also builds peer support networks, enabling women to share experiences and strategies for digital self-defence. Safe Sisters plays a crucial role in bridging the digital literacy gap, particularly for women in underserved communities (Internews, nd).

CyberSafe Foundation's Cybersmart Women initiative

The CyberSafe Foundation's Cybersmart Women initiative focuses on educating women on online safety, particularly those in marginalised communities who are at greater risk of digital abuse. The programme provides accessible training on cybersecurity best practices, helping survivors navigate online spaces securely while advocating for broader digital rights awareness. By fostering community-driven awareness campaigns, the CyberSafe Foundation ensures women have the tools to defend themselves against TFIPV and other forms of online gender-based violence. The initiative also partners with tech companies and law enforcement agencies to improve digital safety resources for vulnerable women (CyberSafe Foundation, nd).

While these initiatives mark significant progress in addressing TFIPV, continued efforts are needed to strengthen law enforcement capabilities, expand legal protections and improve digital literacy programmes, particularly in marginalised communities. A holistic, survivor-centred approach – integrating legal, educational and technological interventions – remains critical to effectively combating technology-facilitated abuse across Africa.

5.2 Recommendations for combating cyberstalking in intimate partner violence

Addressing cyberstalking within the context of IPV in Africa requires a multi-faceted, evidence-based and policy-driven approach that includes legal reforms, digital literacy initiatives, victim support structures, industry accountability and international co-operation. However, to move beyond broad recommendations, specific, actionable steps are necessary to guide policy implementation, technological solutions, funding mechanisms and specialised training programmes for stakeholders.

The following recommendations present a robust and sustainable framework to combat TFIPV.

5.2.1 Strengthening legal frameworks

Enacting IPV-specific cyberstalking legislation

African governments should introduce laws that explicitly criminalise cyberstalking within IPV cases, recognising digital coercive control methods like spyware, GPS tracking and non-consensual sharing of intimate images. These laws should impose strict penalties for unauthorised access to personal devices and online accounts used for abuse. Legal reforms should also mandate technology companies to co-operate with law enforcement in IPV-related cyberstalking cases and integrate specific protections for IPV survivors to prevent abusers from exploiting legal loopholes (Aderibigbe, 2021).

Enhancing enforcement through specialised training

To improve enforcement, governments should implement mandatory, specialised training programmes for law enforcement officers to identify, investigate and prosecute digital abuse cases. Judicial personnel should be trained to understand the intersection of IPV and technology-facilitated abuse. Digital forensic teams should receive advanced training in handling digital evidence in IPV cases. Public–private partnerships should support these training initiatives, with contributions from technology firms and civil society organisations (Nkosi, 2022).

Establishing cross-border legal co-operation

Cyberstalking laws should be harmonised across African jurisdictions to address the borderless nature of digital abuse. Countries should develop extradition agreements for IPV-related cyberstalking offenders and establish cross-border data-sharing protocols to facilitate access to digital evidence. Regional cybercrime taskforces under the AU should be developed to track and dismantle online IPV-related abuse networks.

5.2.2 Digital literacy and victim support mechanisms

Creating multilingual digital safety resources

Governments, non-governmental organisations and technology companies should collaborate to develop and distribute multilingual, culturally relevant digital safety materials. These resources should educate IPV survivors on securing personal devices, recognising spyware and using digital privacy tools. Ensuring accessibility in rural and underserved areas is essential, with resources provided in audio-visual formats for individuals with low literacy levels (Mwangi and Otieno, 2021).

Expanding and funding IPV support networks

IPV survivors need comprehensive, technology-sensitive support services, including 24/7 digital abuse hotlines and online safe spaces. Free digital security clinics should be established to assist survivors in removing spyware and securing devices. Governments should establish sustainable funding mechanisms, including public–private partnerships with technology companies, national budget allocations and international donor grants to ensure long-term financial sustainability.

5.2.3 The role of technology companies in safeguarding users

Strengthening privacy and security features

Technology companies must enhance platform security to protect users from IPV-related cyberstalking. This includes implementing stronger encryption, account security measures, automatic alerts for suspicious activity and easy-to-use account recovery processes for IPV survivors facing cyber threats.

Enhancing reporting mechanisms for IPV-related abuse

Companies should develop user-friendly, multilingual reporting channels that allow IPV survivors to report abuse discreetly. Platforms should offer real-time assistance from digital safety specialists and provide anonymised legal resources for survivors seeking justice.

Collaborating with law enforcement and advocacy groups

Technology firms should work with law enforcement agencies and IPV advocacy groups to improve protection measures for survivors. This includes facilitating priority access to digital security assistance, implementing secure information-sharing protocols and supporting funding initiatives for legal and psychological assistance to victims of digital abuse.

5.2.4 International co-operation and policy implementation

Developing regional and global cyberstalking agreements

African governments should establish intergovernmental task forces under the AU to address cross-border IPV-related cybercrime. Standardised legal frameworks for online IPV prosecution should be developed to ensure uniformity in law enforcement responses. Partnerships with global cybersecurity organisations should be pursued to enhance access to digital crime expertise and technological resources.

Implementing clear policy action plans

Governments should develop clear implementation roadmaps to ensure accountability and measurable progress. This includes assigning responsible agencies for enforcing IPV-related cyberstalking laws; setting time-bound targets for legal reforms, technology upgrades and funding allocation; and establishing monitoring and evaluation mechanisms to assess the effectiveness of implemented policies.

6. Conclusion

The digital age has introduced new dimensions to IPV, particularly through cyberstalking, online harassment and digital surveillance. As technology becomes more integrated into daily life, abusers have new tools to control, manipulate and intimidate their partners. This study highlights the vulnerabilities of victims and the inadequacies of legal systems, digital platforms and social services in addressing technology-facilitated abuse. It explores the legal, social and psychological dimensions of digital abuse and provides actionable recommendations to address these issues.

The findings underscore the need for stronger legal frameworks tailored to digital abuse in IPV contexts. While some African countries have made progress by implementing cybercrime laws and anti-stalking provisions, these laws often remain inadequate in addressing the nuances of digital IPV. Lack of enforcement, limited resources within law enforcement agencies and insufficient public awareness contribute to the continued prevalence of cyberstalking and digital harassment in abusive relationships. Many legal systems lack the capacity to handle the technicalities of technology-facilitated abuse, leaving victims without sufficient recourse.

In addition to legal reform, enhancing digital literacy and providing robust support for victims of cyberstalking are essential steps towards mitigating the impact of digital IPV. Victims often face significant barriers, including a lack of awareness of their rights, limited knowledge of how to protect their digital privacy and social stigmas that prevent them from reporting abuse. Empowering individuals, particularly women and marginalised groups, with the tools to recognise and resist online abuse is key to breaking the cycle of control and manipulation enabled by technology.

The role of technology companies is also crucial in preventing and responding to digital IPV. While many tech companies have implemented safety features, these measures remain insufficient in preventing cyberstalking and ensuring user privacy. There is an urgent need for stronger privacy protections, proactive abuse detection and collaboration between tech companies, law enforcement and advocacy groups. Creating a more user-centred, safety-oriented environment can help the tech industry reduce its role as an enabler of IPV.

Artificial intelligence (AI) introduces additional complexities to the landscape of digital IPV. AI can be exploited by abusers to enhance surveillance, automate harassment and manipulate digital environments. For instance, AI-driven tools can be used to track victims' online activities, generate deepfake content or deploy automated bots for continuous harassment. Future research should explore the implications of AI in exacerbating digital abuse and develop strategies to counteract these threats. This includes advocating for AI ethics in technology development, implementing robust AI detection and mitigation tools, and ensuring AI systems are designed with abuse prevention in mind.

Finally, international co-operation is necessary to address the cross-border nature of cyberstalking. As the internet transcends national borders, abusers and victims of digital abuse often reside in different countries, complicating efforts to prosecute and hold offenders accountable. Strengthening legal co-operation between African countries and beyond, while establishing international norms for digital abuse, will ensure cyberstalking abusers can be held accountable, no matter where they are located.

In conclusion, addressing cyberstalking within IPV requires a multi-dimensional approach involving legislative reform, victim support, digital literacy and industry accountability. African nations must commit to reforming and harmonising legal frameworks, enhancing digital literacy and fostering collaboration between stakeholders to protect IPV victims from technology-facilitated abuse. A co-ordinated, comprehensive response can help mitigate the risks posed by cyberstalking, protect survivors and create a safer, more supportive digital environment. Future writing should delve deeper into the role of AI in digital abuse, exploring both the challenges it presents and potential solutions to safeguard victims in an increasingly AI-driven world.

References

Adebayo, T. and Musa, S. (2021) 'Digital Abuse in Nigeria: The Role of Cyberstalking in Intimate Partner Violence'. *Journal of African Media Studies* 13(2): 89–105.

Adeoye, A. (2024) 'Meta Removes over 63,000 Fake Nigerian Instagram and Facebook Accounts Tied to Scams'. *Financial Times*, 26 August. https://www.ft.com/content/42caef4f-c6d5-41e5-8e91-9b5bebc37b13

Aderibigbe, A. (2021) 'Digital Intimate Partner Violence in Nigeria: Challenges and Interventions'. *Journal of African Studies* 58(3): 221–236.

Adeyemi, A. (2018) 'Cybercrimes and the Nigerian Legal System: Challenges and Opportunities'. Lagos: *Nigerian Law Review*.

Baker, L. and Stonard, K. (2021) 'The Impact of Technology on IPV: A Psychological Perspective'. *Journal of Domestic Violence Studies* 16(2): 81–98.

Bakibinga, P. (2022) 'Cybercrime and Governance in Africa: Evaluating the Implementation of the Malabo Convention'. *African Journal of Law & Technology* 7(1): 45–62.

Bowlby, J. (1969) 'Attachment and Loss: Vol. 1. Attachment'. *New York: Basic Books*.

Chigbu, U., Ezeh, C. and Nnadi, N. (2020a) 'Addressing Cyberstalking in African Societies: Legal and Social Implications'. *African Journal of Cyber Law* 12(1): 15–32.

Chigbu, U., Okoro, P. and Nwankwo, E. (2020b) 'Digital Divide and IPV: The Role of Technology in Rural and Urban Settings in Africa'. *International Journal of Cyber Criminology* 14(2): 233–247.

Collins, J. (2024) 'Nigerian Man Extradited to the U.S. over Sextortion Case Linked to South Carolina Teenager's Death'. AP News, 27January. https://apnews.com/article/832b99698558ccc37beb80d15ea4d83b

Cowan, A. and Boyle, P. (2019) 'Psychological and Emotional Abuse in Intimate Partner Violence: The Role of Technology'. *Journal of Abuse and Trauma* 14(4): 183–205.

CyberSafe Foundation (nd) 'Cybersmart Women Initiative: Empowering Women Against Digital Violence'. www.cybersafefoundation.org (accessed 15 February 2025).

Department of Home Affairs (2021) 'The Cybercrimes Act in South Africa: Implementation Challenges and Prospects'. Pretoria: Government Printer.

Douglas, H., Harris, B.A. and Dragiewicz, M. (2019) 'Technology-Facilitated Domestic and Family Violence: Women's Experiences'. *British Journal of Criminology* 59(3): 551–570.

Dragiewicz, M., May, P.J. and Mohr, G. (2019) 'Technology-Enabled IPV: A Study of Cyber Abuse in Intimate Relationships'. *Violence Against Women* 25(6): 659–677.

Ekanem, S. (2024) '10 Major Cyberattacks That Targeted African Organizations in 2024'. Business Insider Africa, 2 January. https://africa.businessinsider.com/local/lifestyle/10-major-cyberattacks-that-targeted-african-organizations-in-2024/qsqgmlq

Eze, P. and Chukwudi, U. (2019) 'Patriarchy and Digital Abuse: An Analysis of Gender Norms in Nigeria'. *African Journal of Gender Studies* 8(1): 45–62.

FEMNET (nd) 'Digital Rights and Gender Justice in Africa'. https://femnet.org (accessed 15 February 2025).

Global Network Initiative (GNI) (2021) 'Annual Report 2021'. Available at: https://globalnetworkinitiative.org/gni-annual-report-2021/ (Accessed: 11 November 2024).

Hinson, L., Mueller, J., O'Brien-Milne, L. and Wandera, N. (2018) *Technology-Facilitated Gender-Based Violence: What Is It, and How Do We Measure It?* Washington, DC: International Center for Research on Women.

International Telecommunication Union (ITU) (2022) 'Measuring digital development: Facts and figures 2022'. Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (Accessed: 11 November 2024).

Internews (nd) 'Safe Sisters Program: Strengthening Digital Security for Women'. https://www.internews.org (accessed 15 February 2025).

Jackson, A. (2024) 'Cyberattack in Kenya Impacts Online Government Platforms'. *Cyber Magazine*, 31 July. https://cybermagazine.com/application-security/cyberattack-in-kenya-impacts-online-government-platforms

Kamau, J. and Njoroge, R. (2021) 'Cyberstalking and Intimate Partner Violence in Kenya: An Emerging Digital Threat'. *Journal of Cyber Policy* 6(1): 112–130.

KICTANet (Kenya ICT Action Network) (2022) 'Annual Report 2022: Advancing Digital Rights in Kenya'. Nairobi: KICTANet.

Mason, A. (2021) 'The Role of Technology Companies in Preventing and Reporting Cyber Abuse'. *Journal of Digital Law and Practice* 2(3): 112–129.

Mba, O. and Nwankwo, E. (2020) 'The NDPR and Cybercrime in Nigeria: Opportunities and Challenges'. *Journal of Cyber Law in Africa* 14(2): 35–50.

Moyo, T. and Nkosi, B. (2020) 'Digital Misogyny: Exploring the Intersection of Gender-Based Violence and Technology in South Africa'. *South African Journal of Social Research* 8(3): 78–94.

Musambi, E. and Inganga, B. (2024) 'Protests Erupt in Kenya over Gender-Based Violence and Femicide'. AP News, 10 December. https://apnews.com/article/4db1006b745e51dbbed5005f664e632b

Mutua, D. (2019) 'Stigma, Reporting, and Gendered Violence in Kenya: Challenges in the Digital Era'. *East African Social Science Review* 12(2): 55–73.

Mwangi, L. and Otieno, J. (2021) 'Social Media and IPV: Emerging Trends in Kenya'. *East African Journal of Social Sciences* 10(4): 35–48.

Njogu, M. (2020) 'Assessing the Impact of the Computer Misuse and Cybercrimes Act in Kenya'. *Kenyan Journal of Law and Technology* 4(1): 33–48.

Nkosi, Z. (2022) 'Exploring the Impact of Cyber IPV in South Africa'. *South African Journal of Gender Studies* 19(2): 50–65.

Nyeko, O. (2023) 'Ugandan Parliament Passes Extreme Anti-LGBT Bill'. Human Rights Watch, 22 March. www.hrw.org/news/2023/03/22/ugandan-parliament-passes-extreme-anti-lgbt-bill

Okafor, C. (2020) 'Digital Harassment in Nigeria: Prevalence and Implications'. *African Journal of Digital Studies* 7(2): 201–219.

Pence, E. and Paymar, M. (1993) 'Education Groups for Men Who Batter: The Duluth Model'. *New York: Springer.*

PIN (Paradigm Initiative) (nd) 'Protecting Digital Rights in Africa: Advocacy for Legal Reforms'. https://paradigmhq.org (accessed 15 February 2025).

Priebe, G., Holmes, D. and Walker, B. (2017) 'Cyberstalking: The Psychological Effects of Digital Abuse'. *Journal of Psychological Violence* 21(5): 112–127.

Rege, A. (2020) 'Cyberstalking Victimization: An Analysis of Behavioral Impacts'. *Journal of Interpersonal Violence* 35(7-8): 1501–1522.

Reed, L.A., Ward, K. and Parisi, D. (2022) 'Technology and Coercive Control in IPV Cases'. *Criminology & Public Policy* 21(2): 389–415.

Seligman, M. E. P. (1975) 'Helplessness: On Depression, Development, and Death'. *San Francisco: W. H. Freeman.*

Smith, L., Brown, R. and Naidoo, P. (2019) 'Online Harassment and Cyberstalking in South Africa: An Empirical Analysis'. *Cyberpsychology, Behavior, and Social Networking* 22(5): 310–317.

Suler, J. (2004) 'The online disinhibition effect', *Cyberpsychology & Behavior*, 7(3), pp. 321–326.

United Nations Population Fund (UNFPA) (2022) 'Annual Report 2022'. Available at: https://www.unfpa.org/annual-report-2022 (Accessed: 11 November 2024).

UNODC (United Nations Office on Drugs and Crime) (2011) *Handbook on Police Accountability, Oversight and Integrity*. Vienna: UNODC.

Wajcman, J. (2004) 'TechnoFeminism'. *Cambridge: Polity Press*.

Watson, R. and Joubert, E. (2022) 'Addressing Digital Harassment in South Africa: A Review of Legal Gaps'. *South African Law Review* 36(1): 75–98.

Watson, M., Pretorius, L. and van der Westhuizen, C. (2022) 'Digital Forensics in IPV Cases: Challenges and Recommendations'. *South African Journal of Criminal Justice* 35(2): 148–165.

WePROTECT Global Alliance (2022) 'Global Threat Assessment 2022'. Available at: https://www.weprotect.org/global-threat-assessment-2022/ (Accessed: 11 November 2024)

WHO (World Health Organization) (2021) *Intimate Partner Violence: Key Facts*. Geneva: WHO.

Woodlock, D. (2017) 'The abuse of technology in domestic violence and stalking', *Violence Against Women*, 23(5), pp. 584–602.

Zouiten, S. (2024) 'Ouahbi Announces Stricter Penalties for Online Harassment, Blackmail in Morocco'. *Morocco World News*, 22 May. www.moroccoworldnews.com/2024/05/362792/ouahbi-announces-stricter-penalties-for-online-harassment-blackmail-in-morocco

About the author

Chioma Andeh is a cybersecurity and ICT governance professional with nearly a decade of experience spanning legislation, cybersecurity consulting, and digital policy, and open source intelligence. She holds a Master's degree in Information Security and is passionate about privacy, data protection, and digital rights, particularly within the African context. As the Team Lead for Communications and Media at WiCyS Nigeria, she actively promotes cybersecurity awareness and policy advocacy, working to strengthen Africa's digital resilience through research, engagement, and strategic communication.