



The Digital Literacy Paradox

Understanding Technology-Facilitated
Violence Against Women and Girls (TFVAWG)
in Africa in the Artificial Intelligence (AI) Era:
Evidence from Nigeria

Sixtus Cyprian Onyekwere
Adeniran Adedeji
Tamsin Bradley

Policy Brief

A collaboration between the Centre for the Study of the Economies of Africa (CSEA), Nigeria, and the Advancement of Equality, Gender and Inclusion Studies (AEGIS) at the University of Portsmouth, United Kingdom.

Date: April 2026



1.

OVERVIEW

Digital safety programming across Africa, and specifically in Nigeria, is often built on the widely held assumption that merely equipping women with digital skills will shield them from online violence. This policy brief, based on the report of the TFVAWG-CSEA-AEGIS project, empirically tests that assumption. The findings reveal a paradox with insightful implications for digital development policies and programming. Using configurational methodologies, specifically Crisp-set and Fuzzy-set Qualitative Comparative Analysis (csQCA and fsQCA), the research reveals that higher digital literacy consistently appears in every pathway leading to TFVAWG, rather than operating as a straightforward protective factor. Hence, constituting a paradoxical situation where the heaviest burden of Technology-Facilitated Violence Against Women and Girls (TFVAWG) falls not on the digitally impoverished but on the digitality literate. Digital literacy was found to combine with conditions such as young age and heavy online presence as a reliable pathway to TFVAWG.



“In this sample, safety is neither produced by accumulating more digital skills no acquiring higher education. Instead, it is produced primarily by being socially situated outside the environments where other women are being victimised or the combination of possessing no university education, low digital literacy and spending little or no time online.”

Furthermore, the damage caused by these violent encounters is rarely isolated. Nearly 80% of affected women reported emotional distress, and over half modified their digital behaviour, actively reducing their online presence. This creates a silencing effect that actively works against the very goals that digital inclusion programmes strive to achieve.

This brief synthesises these critical findings and provides targeted, strategic recommendations for Nigerian policymakers, NGOs, and international stakeholders. A pivot is urgently required, from focusing solely on individual capacity-building towards structural interventions and rigorous platform accountability.

Practical Takeaway

Readers may be tempted to read the QCA results as the most important part of the study. The QCA results are important, but the practical takeaway from the brief is much simpler than the statistics suggest. Nigerian women are being targeted online, in large numbers, and the response system around them is not working at the level it needs to. Having higher education degrees and being digitally literate are not protecting them. The policy and programming work that flows from this finding is achievable, and it is largely a matter of doing the things that the institutional architecture already permits and doing them with the right unit of focus.

Key Figures from the Study:

Women who reported at least one form of online violence in the past 12 months	63.90%
Affected women who said they felt emotional distress afterwards	79%
Affected women who said it affected their education, work or income	44%
Affected women who reported the incident to police	1%
Women who had received online safety training	58.90%
Women who knew what to do when presented with risks online	41.60%

1.1 Objectives and Study Context

Nigeria is now the largest internet market on the continent, with around 170 million mobile connections ([Garcia-Hombrados et. al, 2024](#)) and over 13 million women online ([USAID, 2023](#)). This expansion has opened educational, economic and social opportunities for women. It has also opened a new front of violence which previous research, conducted mostly for the Global North, has not addressed within African settings. The [Global Solutions Initiative \(2025\)](#) describes a widening digital safety gap for women in the Global South, and the available African evidence suggests that Nigeria sits squarely within that gap.

At the same time, the rapid rollout of generative artificial intelligence has changed what is possible in online violence. Forms of harm which were technically demanding only a few years ago, such as deepfake sexual imagery and coordinated bot harassment, are now within the reach of any user with basic technical knowledge. [UNESCO \(2023\)](#) refers to this as the participation paradox, where the conditions which expand women's digital opportunities are the same conditions which expand their exposure to harm. Phase 2 of the CSEA, AEGIS and GRAIN project was designed in part to test whether this paradox shows up in a Nigerian setting. Hence, this policy brief was intended to reveal the state of TFVAWG in Nigeria and its drivers and, by extension, provide evidence-based recommendations for policymakers, NGOs and other stakeholders on pathways to creating safer digital spaces for women and girls in Nigeria





2.

CONCEPTUALISING TECHNOLOGY FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS (TFVAWG)

TFVAWG: a working definition

Technology-Facilitated Violence Against Women and Girls (TFVAWG) describes different forms of violence, harassment, exploitation, and intimidation directed at women and girls using digital technologies such as mobile phones, social media platforms, and artificial intelligence ([Hinson et al., 2019](#)). In this brief, the terms '**online** violence', '**digital violence**' and 'technology-facilitated violence' are used interchangeably to refer to such acts. .



While both men and women experience online harassment at the empirical level, a targeted focus on Women and Girls is analytically necessary because the underlying generative mechanisms are fundamentally different ([Dune, 2020](#)). The digital violence men face is typically linked to generalised trolling or professional disputes, whereas TFVAWG is driven by deep-rooted patriarchal structures that seek to control women's bodies and police their public participation ([Harris & Vitis, 2020](#)). Viewing this through a socio-ecological lens reveals that TFVAWG is not an isolated digital phenomenon but a direct continuation of offline gender-based violence that leverages women's specific structural vulnerabilities ([Benitz-Hidalgo et.al, 2026](#)), necessitating a dedicated methodological focus to accurately map and address these distinct harms.

To understand the severity of this issue, it is important to view it through a regional lens. Across SubSaharan Africa, an estimated 28% of women have experienced online gender-based violence ([Iyer, Nyamwire & Nabulega, 2020](#)).

Country-specific data reveals even sharper realities: in Uganda, 49% of women report experiencing online harassment over their lifetimes ([UN Women](#)), while in Kenya and South Africa, approximately 33% of internet users report some form of online abuse ([SVIR, 2025](#)). The risk is particularly acute for specific subgroups; for instance, among Sub-Saharan African university students, 64.9% report facing psychological violence and 63.7% experience stalking ([Owusu-Antwi et al., 2021](#)). Furthermore, women in public-facing roles face severe targeting, with 46% of female parliamentarians across 50 African countries reporting online sexist attacks ([Womankind, 2025](#)) and 73% of women journalists globally, including in Africa, experiencing online violence ([UNESCO, 2025](#)). This data demonstrates that TFVAWG is a systemic, continent-wide challenge rather than a uniquely Nigerian phenomenon.

2.1 The Prevailing Digital Policy Landscape and the gaps

Three key existing laws in Nigeria already provide a legal foundation for responding to online violence against women. The [Violence Against Persons \(Prohibition\) Act 2015](#) provides a legislative framework for addressing many forms of violence against women, including cyberstalking. The [Cybercrimes \(Prohibition, Prevention\) Act 2015](#), on the other hand, criminalises sextortion, while the [Nigeria Data Protection Act 2023](#) gives the Nigeria Data Protection Commission the mandate to investigate the unauthorised processing of personal data, which includes non-consensual intimate imagery and AI-generated content built on a woman's resemblance. Yet, despite these legal provisions, enforcement remains limited in practice. Many support services are still concentrated in urban centres, and the content moderation and takedown systems used by major digital platforms often operate beyond the reach of national legal mechanisms.

Moreover, [USAID \(2023\)](#) and the [NITDA National Digital Literacy Framework \(2023\)](#) both rely on the assumption that improving women's education and digital skills will reduce their exposure to online harm. However, as [Livingstone & Helsper \(2010\)](#) established, access to new opportunities and vulnerabilities increase together on the same ladder. If safety competencies do not evolve concurrently with digital access, increased participation guarantees increased victimisation.

Although the [NITDA framework](#) includes online safety as one of its six competency areas, alongside device operation, information literacy, communication, content creation, and problem-solving, safety is still treated as one component among many rather than as a stand-alone national priority. This brief, therefore, examines whether the assumption behind current policy holds true in practice. Specifically, whether digital literacy on its own provides the level of protection policymakers expect for Nigerian women online.

Addressing this growing threat requires well-grounded legal frameworks, and various efforts are underway across the continent to close the legislative gap. At the continental level, the AU Convention on Ending Violence Against Women and Girls (AU-CEVAWG), adopted in February 2025, provides a comprehensive framework that explicitly includes online platforms, though it requires member state ratification to become legally binding ([AU, 2025](#)). Similarly, the Malabo Convention on Cybersecurity and Personal Data entered into force in 2023, though it suffers from limited ratification and has been criticised for vague language ([AU, 2024](#)). Regionally, ACHPR Resolution 522 calls on states to expand the definition of GBV to include digital violence, but as a non-binding resolution, civil society reports its implementation remains weak ([CIPESA, 2025](#)). At the national level, some countries are making targeted legislative strides: Ghana's Cybersecurity Act (2020) is considered a leading example for explicitly criminalising the nonconsensual sharing of intimate images with up to three years in prison ([IFEX, 2025](#)). Likewise, South Africa's Cybercrimes Act (2021) outlaws the non-consensual distribution of intimate images, and Kenya's Computer Misuse and Cybercrimes Act (2018) addresses cybercrimes broadly; however, across all these national examples, effective enforcement remains a major and ongoing challenge.



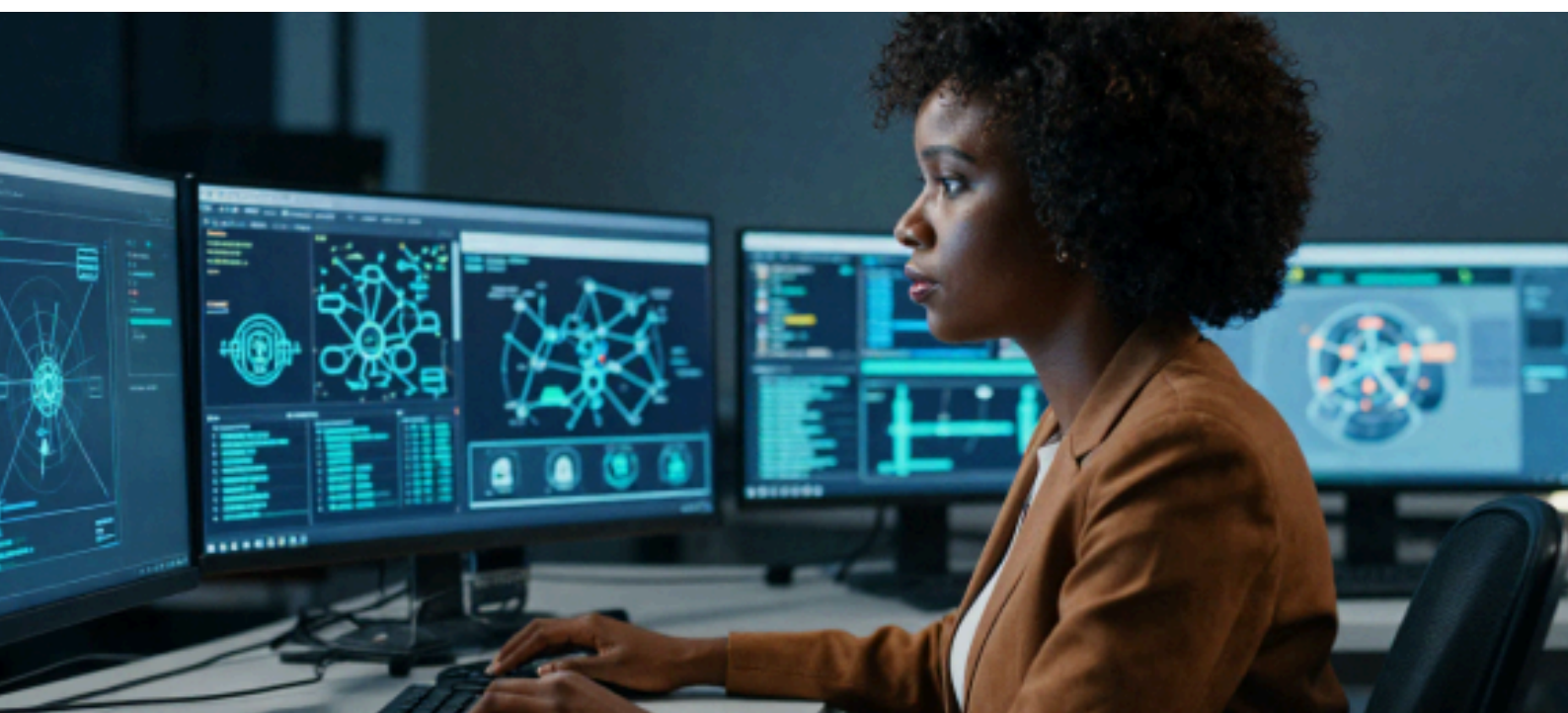


3.

STUDY DESIGN

This brief is based on results from a cross-sectional online survey of women in Nigeria. The survey was conducted between December 2025 and March 2026 and distributed via the social media channels of the Centre for the Study of the Economies of Africa (X, LinkedIn and Facebook) with ethical approval provided by the University of Portsmouth through the AEGIS Centre collaboration (ethics reference: FHSS 2025089). A total of 301 valid responses were collected, and after data cleaning, 283 responses were retained for final configurational analysis. Because participation was online and recruitment followed a nonprobability approach, the sample is more reflective of younger, urban, digitally active women, particularly from southern Nigeria. As a result, the prevalence figures presented in this brief should not be interpreted as representing the full scale of TFVAWG in Nigeria. If anything, they are more likely to underestimate the extent of the problem.

It may be argued that because the sample is biased towards younger, urban, southern and digitally active women, the results of the study are not suitable for policy. However, the relevant question for policy is not whether the sample is unbiased in the statistical sense, but whether the women who appear in the sample are the women whom the existing policy is designed to serve. The sample is, in fact, composed of exactly the kind of women whom current digital literacy and education programmes are most likely to reach. If the protective assumption/programmes fail for this group, then it is unlikely they will hold for women with less education and less digital exposure. The findings should therefore be read as a lower bound for the policy challenge, not as a marginal case.



3.1 Data Analysis: Why QCA?

The analytical strategy combined descriptive statistics, cross-tabulations and Qualitative Comparative Analysis (QCA). QCA was preferred to formal regression for its usefulness in addressing social outcomes that result from complex intersection patterns. There has been broad consensus among scholars and practitioners that violence against women and girls is a systemic phenomenon that results from the intersection of multiple factors rather than from the impact of one single variable ([WHO, 2024](#)). From this reasoning it is apparent that while standard regression modelling approaches that separate the impact of individual variables are useful, they are not equipped to explain how multiple configurations of conditions (factors) interact to cause or negate a given outcome. QCA was developed specifically to achieve this purpose. Again, unlike traditional regression modelling approaches, QCA performs well under small sample sizes and does not require random sampling ([Marx et al., 2014](#)). These uniquely position QCA as the best method for sensitive studies such as this (i.e., with a small sample size and where the outcome is better framed as resulting from a combination of intersecting conditions).

Furthermore, the study gathered data through online surveys where people volunteered, which naturally creates a 'selection bias'. Bias in this sense arises as survivors of severe violence might be less likely to participate, and participants who did not have internet access at the time of the survey or see the call for participation were also unable to participate. Hence, as noted earlier, data were skewed towards demographics. Unlike traditional regression, which relies on perfectly random samples (unbiased) to make broad estimates about a whole population, the method used here (QCA) does not rely on a perfectly random sample, and it is not tied to making population-level claims ([Marx et al., 2014](#)). Instead of trying to predict or generalise to the whole population (like in regression modelling), QCA focuses on the specific number of people (cases) in the study and systematically assesses how different conditions (factors) combine in their specific lives to create risk or safety ([Thomann et al. 2017](#)). Simply put, it is a bridge between qualitative assessment and quantitative analysis which uses systematic pattern matching through set theory and Boolean algebra. Hence, selection.

The study deployed two types of QCA; Crisp-set QCA and Fuzzy-set QCA. Following the same approach used in [Lambert and Krivokapic-Skoko \(2016\)](#), the study first applied crisp-set QCA (csQCA) to assess the configurational combinations of conditions that lead to TFVAWG. 'Crisp-set' in this sense refers to the use of data in binary forms (such as YES/NO).

For example, a question may require a participant to choose either 'educated' or 'not educated'- no middle ground. Essentially the condition is either fully present (1) or fully absent (0). The next step taken moved beyond Crisp to fsQCA

Fuzzy-set QCA (fsQCA) refined the analysis by introducing graded membership, allowing variables to have middle grounds (i.e., take any values between 0 and 1). For example, instead of educated (1) Vs uneducated (0) as used in Crisp-set, the variable in fuzzy set is graded from lower to higher ordinal ranking, such as no education (0), Primary school (0.2), Secondary school (0.5), and up to university level (1), which is more realistic. This recognises that some conditions may lose meaning if tightly forced into a YES/NO ([Dul, 2016](#)). For example, digital literacy assessment is better represented by a formulation that allows answers with degrees of difference, such as 'NO digital literacy', 'Low digital literacy', 'High digital literacy', etc., instead of simple 'Yes/NO' answers that eliminate the possibility of partial knowledge of digital literacy. Likert scale-type examples (strongly agree... to strongly disagree) are a perfect example of the logic of fsQCA due to their adherence to the logic of partial presence (i.e., conditions with degrees of difference).

The use of these two QCA approaches in this study helped with robustness (i.e., to gauge whether results remained the same or shifted under different analytical conditions).



3.2 Variable Measurement and Key to Understanding QCA Results

The configuration analysis included specific conditions such as age (AGE), Education level (EDU), online exposure (EXP), Digital literacy (DL), Online safety competence (SAF), and whether the respondent knows anyone who is a survivor of TFVAWG (PEER). The conditions were selected in line with existing theories ([see Prensky, 2001; Hunsaker & Hargittai, 2018; Livingstone & Helsper, 2009; Lissak, 2018; Dunn, 2020; Powell, Flynn & Sugira, 2021](#)). Other demographic and behavioural variables were included for wider context on coping and the impact of TFVAWG. On the outcome dimension, the study assessed both overall TFVAWG and AI-enabled VAWG.

- The result from QCA is read as a configuration that led to the outcome. For instance, you may find that one hand, participants reporting high TFVAWG hold the profile of primary education, high digital literacy and low online safety knowledge. On another hand, another group of participants who also reported high TFVAWG may hold a different profile, such as low digital literacy, urban residence, low online exposure, and so on. Hence, QCA shows different pathways that lead to the same outcome, which is called ‘equifinality’ ([Dul, 2016](#)). This earns QCA a recognition among critical realists as a methodology for understanding systemic and structural issues in societies ([Gerrits and Verweij, 2015](#)).

The result from QCA is read as a configuration that led to the outcome. For instance, you may find that one hand, participants reporting high TFVAWG hold the profile of primary education, high digital literacy and low online safety knowledge. On another hand, another group of participants who also reported high TFVAWG may hold a different profile, such as low digital literacy, urban residence, low online exposure, and so on. Hence, QCA shows different pathways that lead to the same outcome, which is called ‘equifinality’ ([Dul, 2016](#)). This earns QCA a recognition among critical realists as a methodology for understanding systemic and structural issues in societies ([Gerrits and Verweij, 2015](#)).



4.

RESULTS

First, descriptive statistics are provided to show prevalence, effects and coping strategies currently being used by participants. This is then followed by the formal fsQCA results showing different risk pathways to TFVAWG, as well as protective pathways

4.1 Prevalence and Landscape of TFVAWG

The analysis is based on a purposive sample of 301 internet-connected women in Nigeria. The findings suggest that TFVAWG is not a rare or isolated experience but a deeply embedded feature of women's digital lives.

63.90%

of Nigerian women in the sample reported at least one form of TFVAWG in the preceding 12 months

Nearly two-thirds of participants (63.9%) reported at least one experience of online violence during the preceding year. This is higher than the prevalence rates reported in similar studies done for neighbouring countries which also utilised small samples. For instance, [Iyer, Nyamwire & Nabulega \(2020\)](#) reported the following: Ethiopia 31.2% (N=487), Uganda 28% (N=720), South Africa 23.3% (N=536), and Senegal 25.5% (N=701). Given Nigeria's status as the fastest growing as well as largest internet market in sub-Saharan Africa, the higher prevalence may be expected.

Moving beyond prevalence, the data from this study also revealed the layered nature of these experiences. Women who reported exposure rarely encountered only one form of abuse. On average, affected participants experienced roughly three different forms of violence, while a smaller group reported exposure to ten or more.

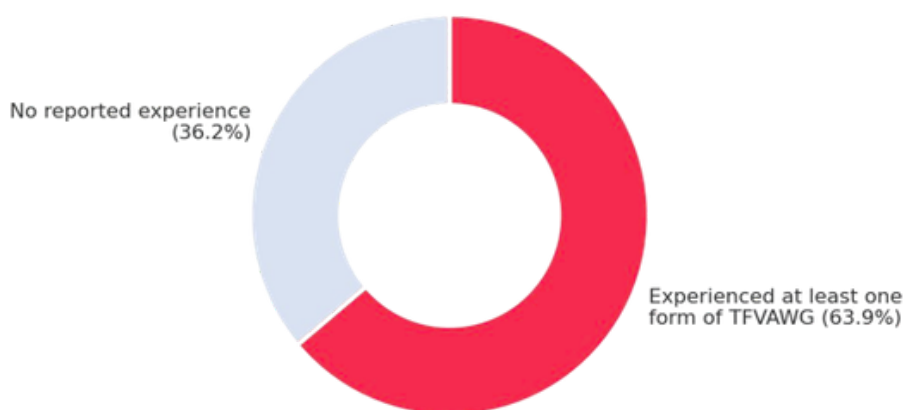


Figure 1. Prevalence of TFVAWG in the preceding 12 months

Accumulation of Harm: Among the affected majority, experiencing multiple forms simultaneously was standard. The average affected participant encountered approximately three distinct forms of violence from the 13 different forms shown in Figure 2.

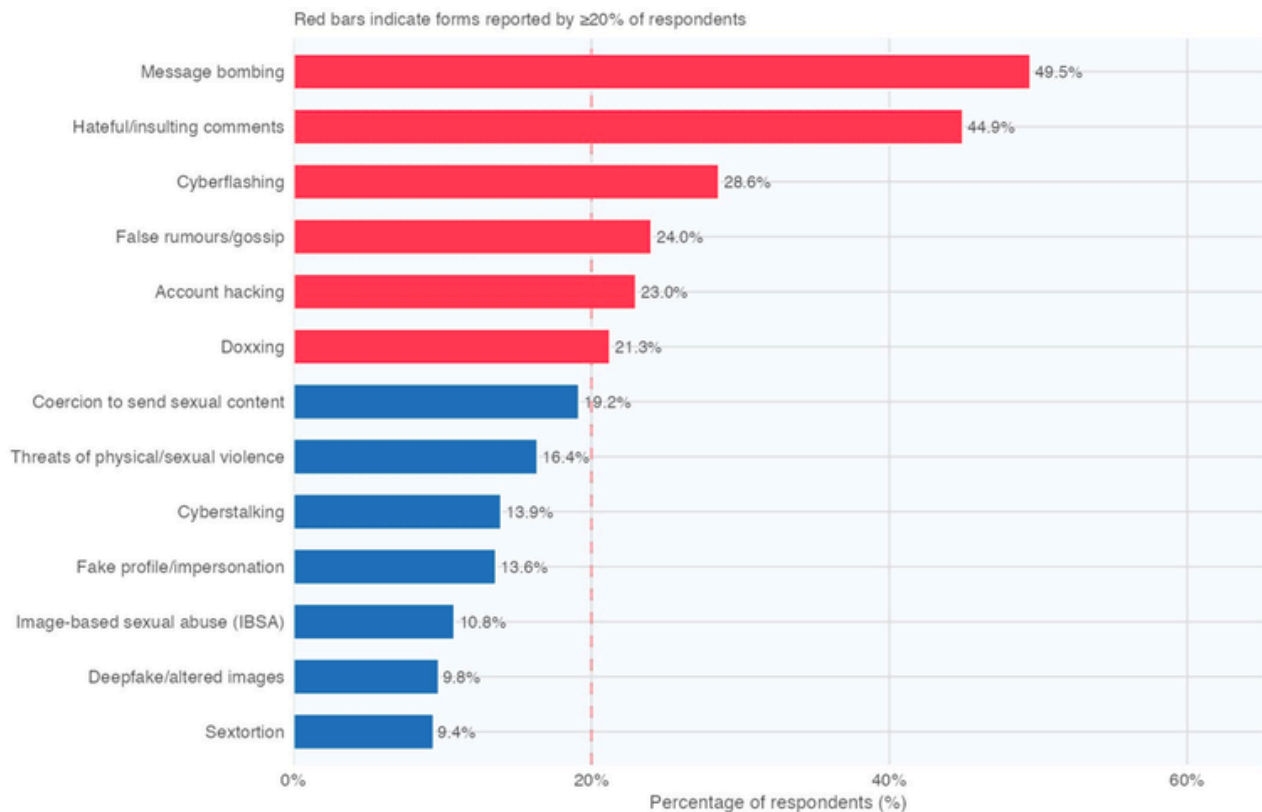


Figure 2. Percentage of participants who experienced specific forms of online violence. Data demonstrates that messaging abuse and hateful comments dominate, while severe privacy violations remain alarmingly prevalent.

4.2 How Digitally Skilled Were Participants (self-reported)?

Participants generally rated themselves as digitally capable. More than 80% said they could search the internet effectively and knew how to block or report abusive accounts. Confidence in cybersecurity and technical troubleshooting was slightly lower but still above the midpoint; this suggests that a lack of basic digital skills does not explain why so many women are targeted.

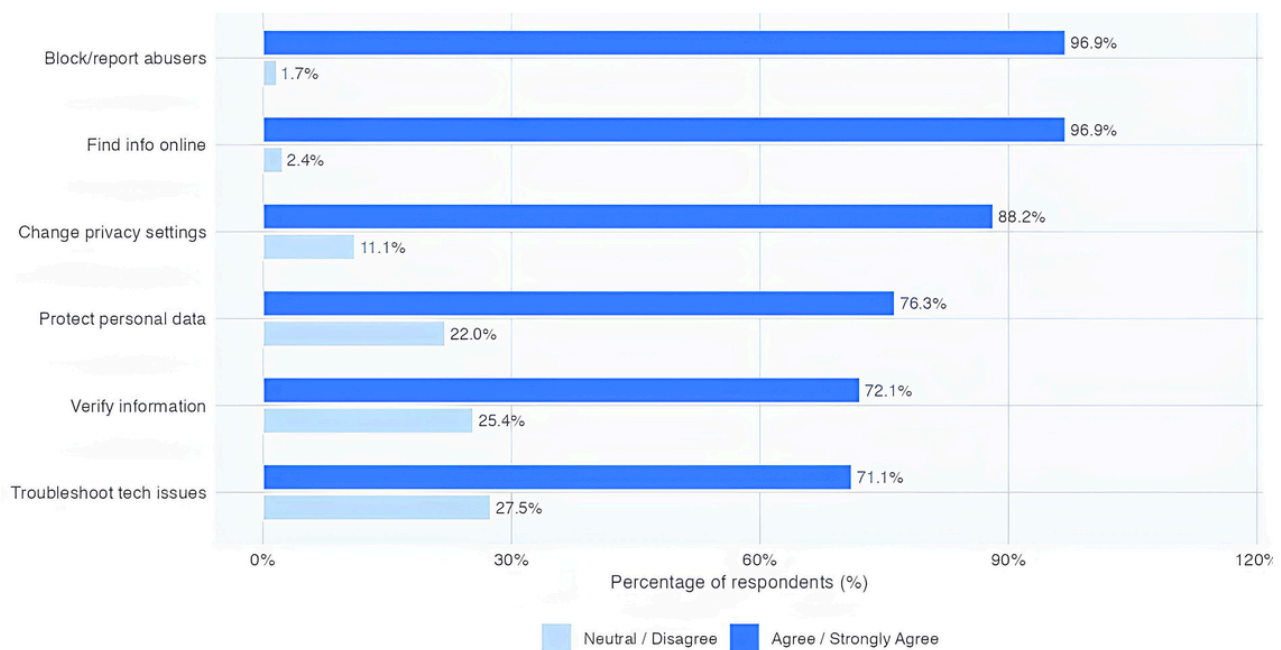


Figure 3. Percentage of participants who agreed or strongly agreed with each digital skill statement

Nevertheless, even though more than half of the survey participants (58.9%) reported that they had participated in some kind of online safety training, less than half of the respondents (41.6%) were aware of what actions should be taken upon coming across any risks on the Internet. It should be emphasised that the difference between these two statistics is significant because receiving training does not necessarily mean knowing how to cope with online risks.

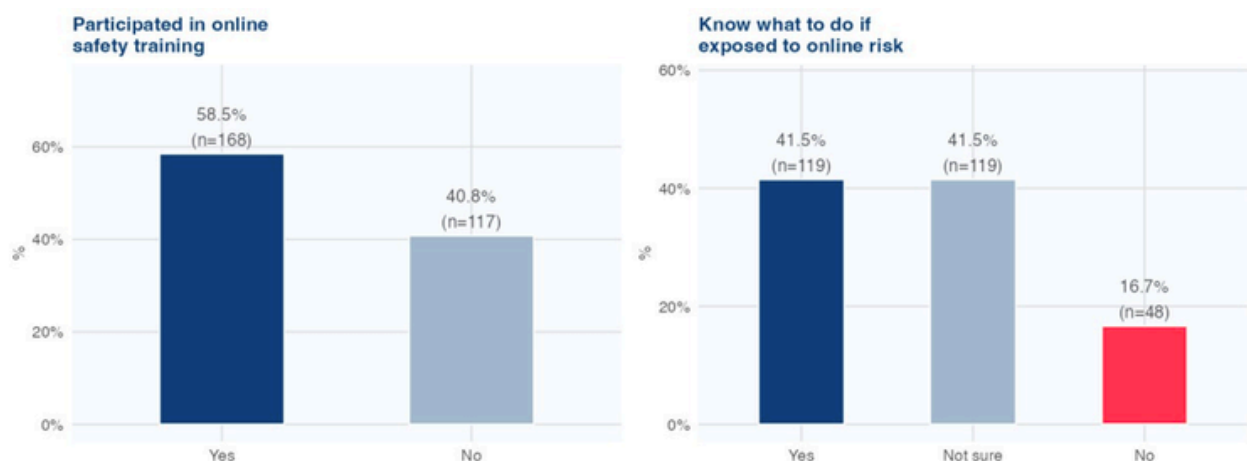


Figure 4. Safety training participation and self-rated safety knowledge (N = 287).

4.3 Unpacking the Risk: A Configurational Approach

In this section, the study turns to the formal assessment of the drivers of TFVAWG through the QCA necessity and sufficiency analysis.

Necessity Analysis:

Schneider and Wagemann (2012) recommend a consistency threshold of 0.90 to support a necessity claim for an outcome. Three conditions sit at or close to that threshold. Younger Age reaches 0.945 for Alenabled TFVAWG and 0.919 for Overall TFVAWG. High Digital Literacy reaches 0.921 and 0.882 across the same two outcomes. Low Safety Competence reaches near necessity 0.897 and 0.823. PEER (awareness of someone who a survivor of TFVAWG is) does not pass the necessity threshold for Overall TFVAWG but plays a strong role in the sufficiency results in next sub-section

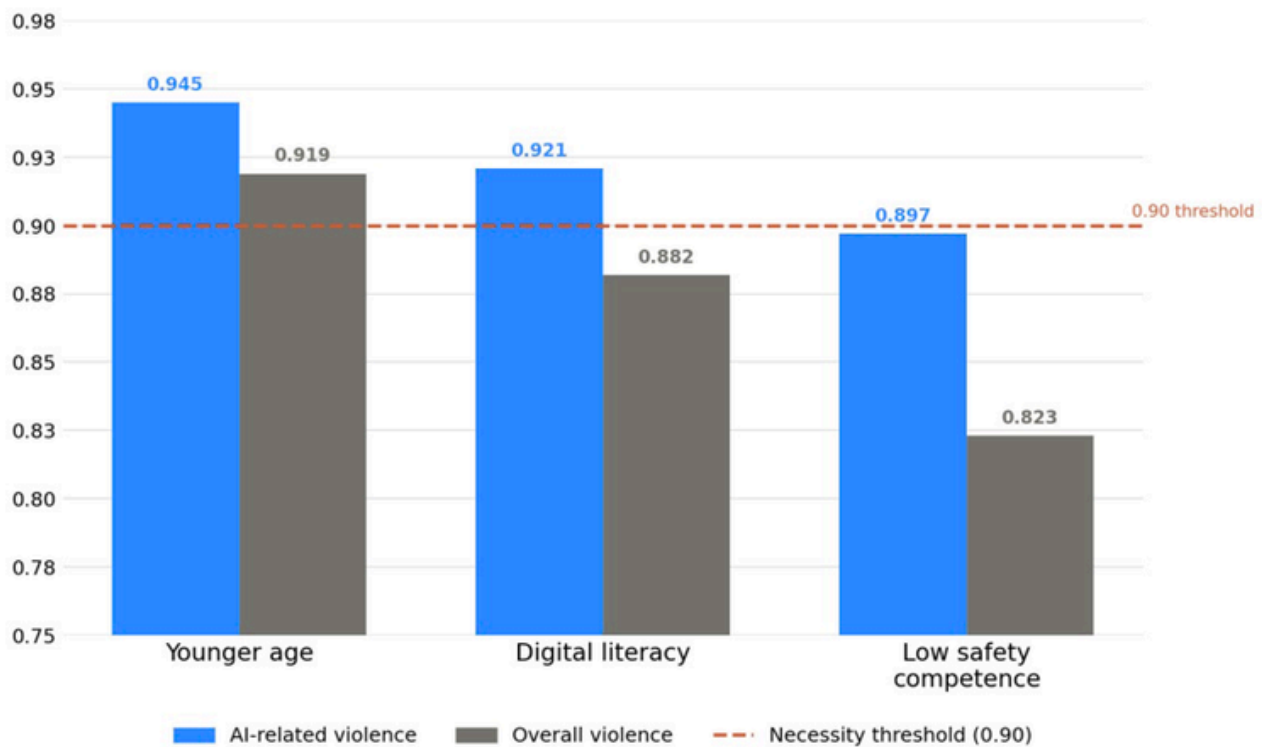


Figure 5. Necessary conditions for TFVAWG

Sufficiency configurations:

The sufficiency analysis shows the combination of factors or pathways for TFVAWG. A condition can be necessary but not sufficient. While younger age and high digital literacy are necessary, they must combine with other conditions as shown in Figure 5 to produce the outcome

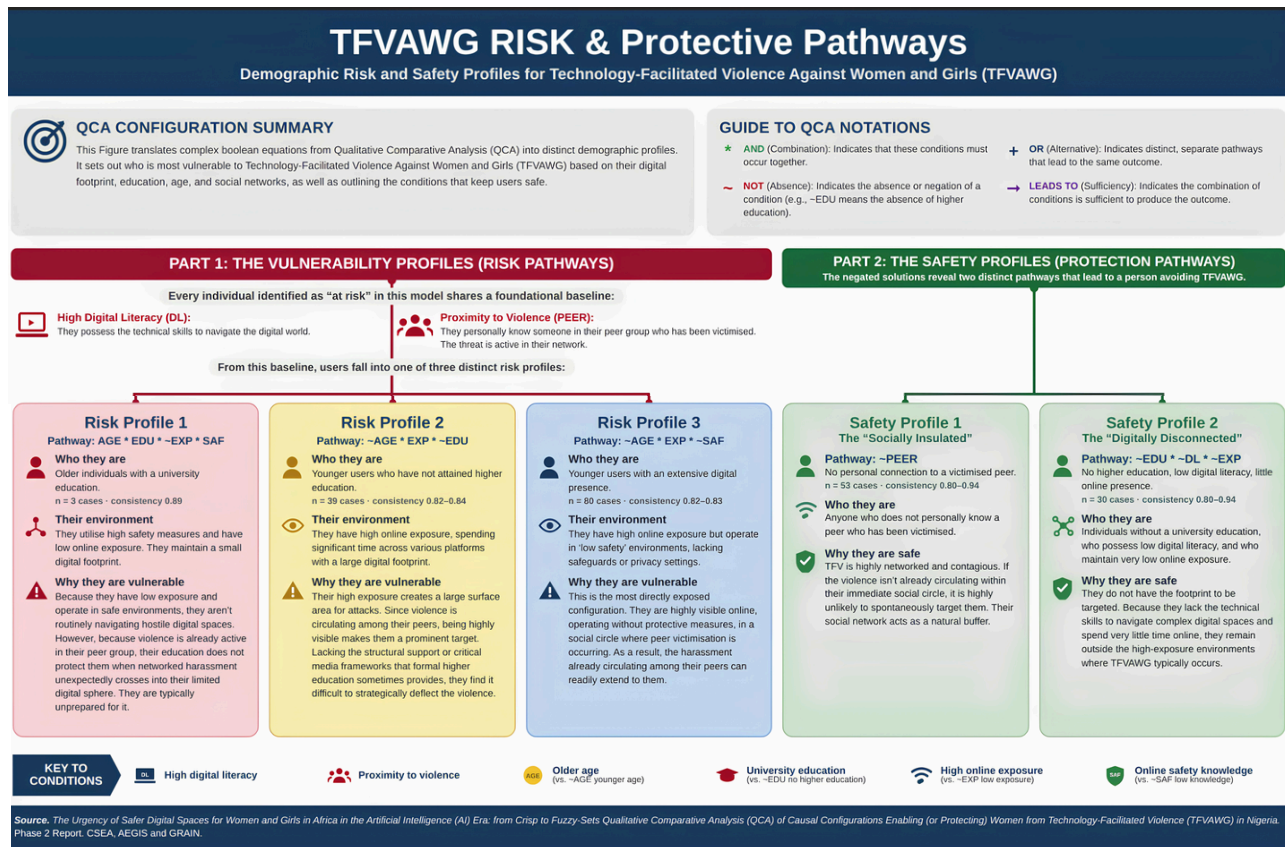


Figure 6. Summary of the configurational pathways for the presence and absence of TFVAWG
Source: Authors' synthesis based on findings

As shown in this section (Fig. 6), one of the prominent findings is that high digital literacy consistently appeared within pathways linked to higher overall TFVAWG exposure and AI-enabled TFVAWG. Rather than functioning as a shield, digital literacy often reflected deeper immersion in online environments where risks were also greater. University education similarly did not eliminate vulnerability and did not appear to matter much in this sample. The analysis for the profile of women reporting no TFVAWG showed two pathways. Either they possessed low digital literacy, limited online exposure and no university degree or they reported no peer victimisation. In other words, safety was shaped more by the social environment surrounding women online than by technical skill acquisition alone. It should be noted that these configurations are reliable combinations of conditions that lead to or negate TFVAWG in the sample, as consistency scores are all well above 0.75.

One key point to be drawn from Fig. 5 for non-governmental organisations and policymakers is that since the groups (risk profiles) differ from one another, a single standard response is unlikely to prove effective, and intervention is better directed at the conditions specific to each group/risk profile.

4.4 The Compounding Human Cost

Statistics on prevalence capture only one part of the story. The consequences that follow exposure reveal the broader social and economic costs of online violence.

Participants were asked to assess the effects of TFVAWG across several domains, including emotional wellbeing, relationships with family and friends, work or education, and willingness to continue engaging online. The responses painted a troubling picture of cumulative harm.

Post-exposure outcomes among the 63.9% of respondents who reported any TFVAWG in the past 12 months



How to read this: the top band shows the wellbeing toll, the middle band shows the economic and social cost, and the bottom band shows what women actually do in response.
The 1% formal-reporting figure is the most important policy signal in the entire study.

Figure 7. Impacts of TFVAWG across domains. Violence forces a direct reduction in digital participation, resulting in acute economic and educational consequences.

Figure 5 summarises every consequence the study measured in three bands. The top band covers the wellbeing toll. About 79% of affected women felt some emotional distress, and roughly 42% described that distress as severe or very severe. Nearly 59% reduced or avoided their online engagement after the incident. About a quarter (25%) reported harm to family or friends arising from what happened to them.

The middle band covers the economic and social toll. About 44% of affected women reported negative effects on their education, work or income. Smaller shares self-censored online (18%), cut their time online (17%), or deleted their account entirely (12%). These are personal costs, and they are also national costs. They show up in silenced women who lost work and lost productive participation in the digital economy.

The bottom band of the figure is the most important policy signal in the entire study. Only about 1% of affected women contacted the police or any government authority. The behaviours women used were blocking the perpetrator (52%), reporting on the platform (32%) and telling a friend or family member (27%). The formal justice route was almost completely absent (1%).

Most alarmingly, 59% of these women said they deliberately reduced or avoided online engagement after their experiences. This withdrawal effect directly undermines the goals of digital inclusion and empowerment. When women retreat from digital spaces to protect themselves psychologically, they also lose access to educational opportunities, economic participation, professional networking, and civic engagement that increasingly depend on online connectivity.

4.5 Artificial Intelligence as an Amplifier

Artificial intelligence introduces a new dimension to gender-based violence online. Rather than representing an entirely separate category of abuse, AI functions as a force multiplier that expands the scale, speed, and reach of harm.

Generative AI tools now make it easier to create non-consensual deepfake imagery, while platform algorithms can rapidly amplify misogynistic or abusive content. Although direct targeting through deepfake technologies was reported less frequently than forms of messaging abuse, the psychological effects extended beyond those personally targeted.

The analysis identified what may be described as a vicarious harm (the psychological damage you experience just by existing in an online community where abuse is common), particularly among younger women operating within peer-victimised environments ([Carlson & Witt, 2020](#)). Even witnessing Alenabled abuse directed at others created anxiety, insecurity, and a sense of vulnerability. Exposure to abuse and harassment created using Artificial Intelligence carried a symbolic threat capable of destabilising women’s sense of safety online, regardless of whether they themselves were directly targeted ([Yavuz, 2025](#)).

Most participants also expressed serious concerns about the future trajectory of AI. Many believed that platform algorithms accelerate the spread of harmful content, while AI voice assistants and related systems often reinforce gender stereotypes rather than challenge them.

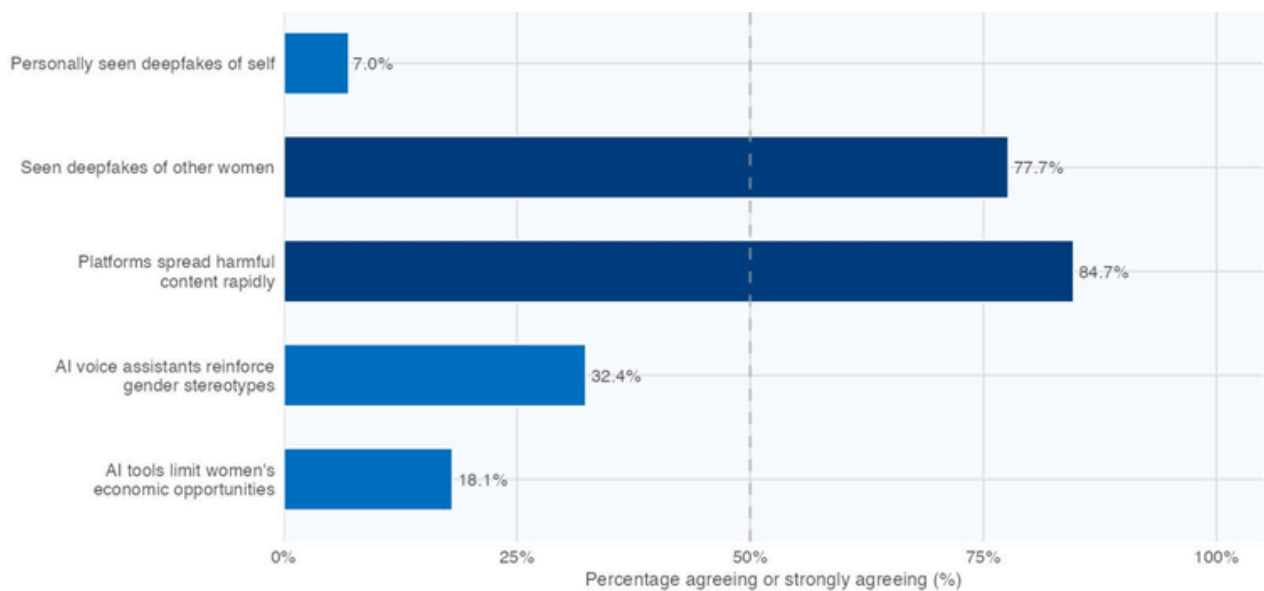


Figure 8. spread of AI harm

4.6 The Deficit of Institutional Trust

How do survivors in Nigeria respond when they experience technology-facilitated violence? The behavioural evidence reveals a striking disconnect between formal legal structures and lived reality.

1%	of affected women contacted the police or any government authority after their TFVAWG experience.
----	---

Despite the existence of the Cybercrimes (Prohibition, Prevention) Act 2015 and the Nigeria Data Protection Act 2023, formal reporting channels are almost entirely absent from survivors' responses. Only about 1% of affected women reported their experience to the police or any government authority.

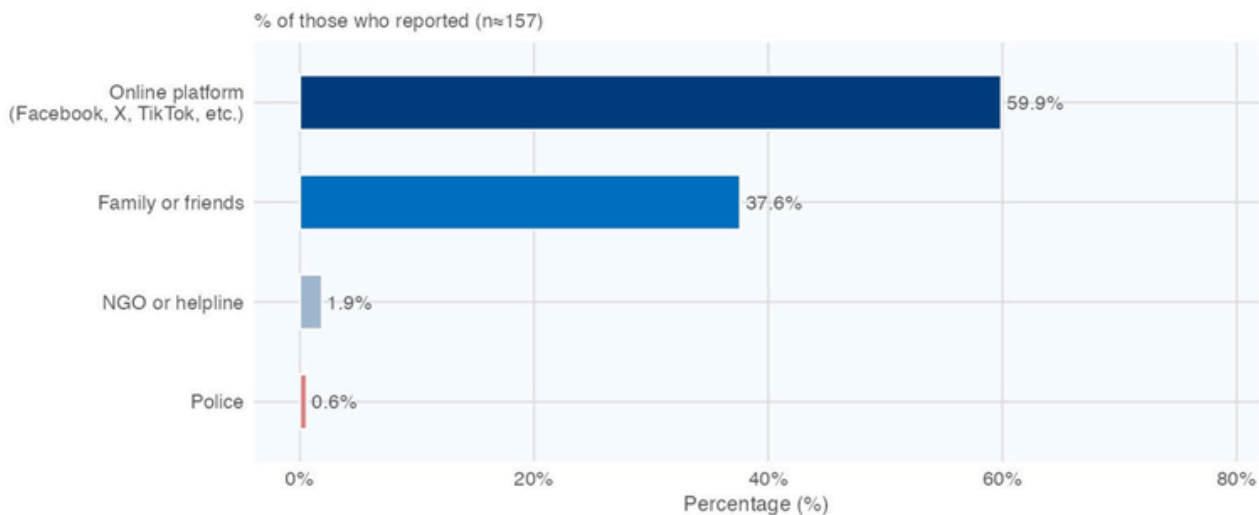


Figure 9. Reporting behaviours among survivors. The near-total absence of formal law enforcement utilization indicates profound institutional distrust.

Instead, survivors overwhelmingly turn to informal and self-managed coping strategies. The most common response is simply blocking the perpetrator (52%), followed by using in-app platform reporting tools (32%). In contrast, seeking help from state institutions remains extremely rare, accounting for only around 1% of reported actions.

This 1% formal reporting rate is not an anomaly to be fixed with awareness campaigns. It is a rational response to an institutional environment perceived as unresponsive, ill-equipped, and fraught with secondary victimisation (Colburn et al., 2023). Survivor-support services built around the reporting pathways that institutions prefer, rather than the pathways women use, will systematically fail.

4.7 The Protective-factor Paradox

17.3PP
Percentage Points

Gap between the share of women who have received online safety training (58.9%) and the share who know what action to take when facing risk online (41.6%).

Higher Education and Digital Literacy are not the safety shield promised. This is the central observation from the study. Higher education and digital literacy, the two factors that current digital-safety programming relies on, are not behaving as protective factors in the Nigerian data. Figure 8 makes the paradox visible in two panels. Panel A shows the 17.3-point gap between training receipt and practical safety knowledge. Panel B compares the three candidate protective factors side by side, and only one of them (practical safety knowledge) behaves like an actual safety shield.

Figure 5. Why education and digital literacy are not the safety shield they look like

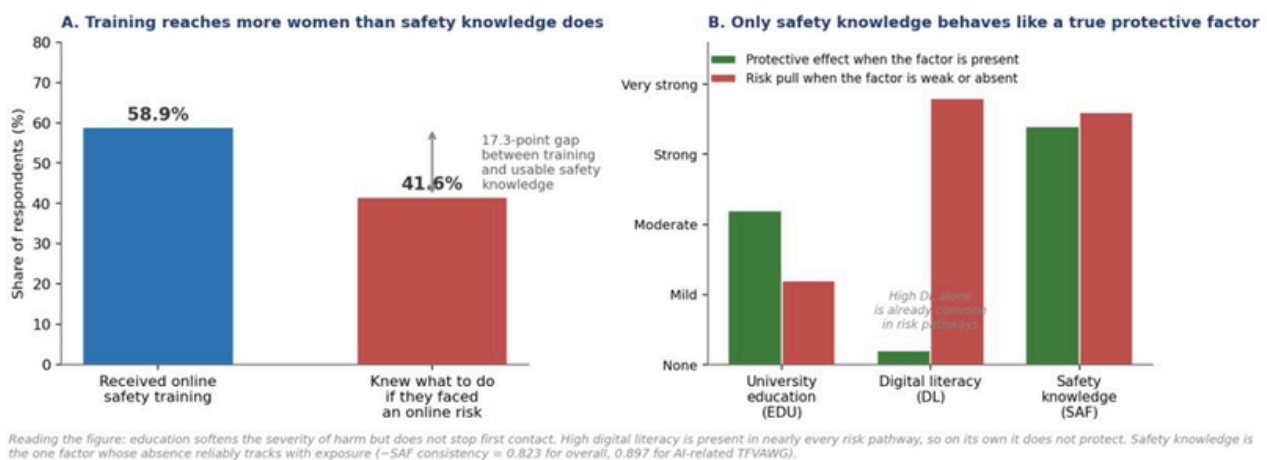


Figure 10. Why education and digital literacy are not the safety shield they look like. Panel A: the training-to-knowledge gap. Panel B: the comparative protective strength of education, digital literacy and safety knowledge.

Among the survey participants, 63.3% had attained a degree or higher level of education, and over 80% reported being able to search for information on the internet, block users and report abuse. Despite these strong digital competencies and high education levels, exposure to TFVAWG remained high. The configurational analysis confirmed that neither education nor general digital literacy operated as a protective factor in any sufficient combination of conditions. Education did appear to limit how severe and how repeated the harm became, but it did not prevent first contact.

High digital literacy appeared in nearly every risk pathway, which means that teaching digital skills without teaching safety knowledge moves women into the digital environment with more confidence than protection. Hence, the participation paradox described by [Chowdhury and Lakshmi \(2023\) at UNESCO](#) therefore moves beyond a theoretical observation about the global digital environment. It shows up in the Nigerian data, and it shows up more strongly for AI-enabled TFVAWG than for the broader category.

What did appear consistently in the analysis was the absence of safety-specific knowledge. While 58.9% of participants had participated in some form of online safety training, only 41.6% knew what actions to take when they came across risks online. The low-safety-knowledge condition reached a consistency value of 0.823 for overall TFVAWG and 0.897 for AI-enabled TFVAWG, which means it sits at or close to the necessity threshold that Schneider and Wagemann (2012) recommend. In plain language, women who do not know what to do when something goes wrong online are the women who end up exposed, regardless of how educated or digitally fluent they are. This is the silence which the curriculum design needs to fix, and it is a curriculum design problem with a curriculum design solution.

41.60%

Participants who knew what actions to take when they came across risks online, despite very high reported digital literacy in the sample



5.

STRATEGIC POLICY
RECOMMENDATIONS

The findings reveal that the current programming logic in Nigeria, and in much of Africa, has been targeting the wrong unit. By focusing on the individual woman and her skill level, programmes have overlooked the peer environment of that woman, the gap between training and practical safety knowledge, and the weakness of formal reporting channels. The four policy directions below follow directly from the findings of this study, and each carry both general TFVAWG considerations and specific implications for AI-enabled TFVAWG, given that AI was found to produce a wider set of pathways into harm than non-AI forms.

- **Shift attention from the individual woman to her environment**

Programmes which focus solely on training individual women are targeting the wrong unit. Community-level responses need to sit alongside individual training. This would include survivor-support groups, peer-education initiatives and content moderation processes which reflect the realities of what women on Nigerian platforms face, including the AI-enabled forms. Agencies such as NITDA and the Federal Ministry of Women Affairs could integrate peer-network mapping into the baseline assessments of the National Digital Literacy Framework. This way, women in high-risk peer environments (including those whose networks show signs of circulating deepfake content) are identified early and offered targeted support, rather than being treated as average users. At the regional level, the African Union Continental AI Strategy (2024) and the Malabo Convention (2014) both push member states to embed gender-specific risk assessment in digital governance, which provides an institutional home for these efforts.

- **Re-scope digital literacy curricula to include safety content**

This brief does not recommend cutting existing digital literacy programmes. The foundational content these programmes deliver is valuable and should be retained. What the brief recommends is that the safety component of these programmes be strengthened, that they include legal-rights content specific to Nigeria, and that they pay more attention to the peer environment of participants. These are additive recommendations rather than substitutive ones. The foundation layer of existing curricula is valuable and should be retained. This includes privacy management, blocking and reporting, and verification of online information. What needs to be added is threat-specific safety content which speaks directly to the Nigerian context. This added content should cover the legal protections available under the [Violence Against Persons \(Prohibition\) Act 2015](#), [the Cybercrimes Act 2015](#) and the [Nigeria Data Protection Act 2023](#), as well as AI-specific safety content covering the identification of deepfake material, the redress pathways available under the Nigeria Data Protection Act 2023 for non-consensual deepfake imagery, and an awareness of how AI-driven harassment campaigns operate. Given the findings, AI-specific safety content cannot be treated as an optional add-on.

The gap between the 58.9% who have received training and the 41.6% who know how to respond is a curriculum design problem, and it has a curriculum design solution. Embedding short, practical safety units inside subjects which students are already studying in (such as journalism, social work, computer science and communication studies or General studies- GST) is likely to produce a larger return than adding a standalone safety module that many students will not take. Where universities are already partnering with platform companies on digital inclusion under the USAID (2023) framework, those partnerships could be extended to cover both general and AI-specific safety content as a shared deliverable.

- **Strengthen the channels women use**

Platforms operating in Nigeria do so under licensing arrangements which the Nigerian Communications Commission already oversees. The Nigeria Data Protection Commission likewise has the mandate to enforce data-related elements under the Nigeria Data Protection Act 2023. Therefore, a possible misconception that platform accountability is beyond the reach of national regulators is not consistent with the existing institutional architecture. What has been missing is the political will to apply these levers specifically to TFVAWG.

Given that only about 1% of participants reported to formal authorities while around 32% used platformlevel reporting, the channel which Nigerian women use is the platform itself. Strengthening this channel means holding platforms accountable rather than simply teaching women to use it more often. Platform companies operating in Nigeria should be required to publish clear data on how quickly they respond to TFVAWG reports, how often they act on them, what appeal processes are available to survivors, and what their detection rate is for AI-generated harmful content directed at Nigerian women, including deepfake material in Yoruba, Igbo, Hausa and Pidgin English. The Nigerian Communications Commission has the licensing leverage to set these requirements, and the Nigeria Data Protection Commission has the mandate to enforce the data-related elements, including the application of the Nigeria Data Protection Act 2023 to non-consensual deepfake imagery cases.

Alongside this, there is a strong case for investment in survivor-support services which do not require any formal reporting, including peer helplines, anonymous support groups and psychosocial care. There is also a parallel case for treating the African language detection capability AI 'N-ATLAS', supported through the joint NITDA and Federal Ministry of Communications initiative, as a national public good, and to strengthen the NITDA-NKENNE AI partnership.

- **Build a regional research base**

The patterns found in this study, especially the dominance of peer environment over individual skill and the wider explanatory footprint of AI-enabled TFVAWG, deserve to be tested in other African settings. A regional research programme applying the same two-stage configurational analysis across different African countries would allow policymakers to assess whether the patterns identified here hold more broadly, and how the AI-enabled component is evolving across countries with different language profiles and platform footprints. The [ECOWAS regional digital agenda](#) and the [African Union Continental AI Strategy \(2024\)](#) both provide institutional homes for such a programme, and any [new federal AI policy in Nigeria](#) should include a gender impact assessment which draws on findings of these types of research.





6.

TRACKING PROGRESS: MONITORING AND EVALUATION

For the recommendations in this brief to be useful, they need to be matched with indicators which can be tracked over time. Table 1 sets out a small set of suggested indicators which government agencies, NGOs and platform companies could adopt to monitor progress on TFVAWG response in Nigeria.

Table 1. Suggested monitoring and evaluation indicators

Indicator	Baseline value from findings	Suggested target
Share of Nigerian women reporting at least one TFVAWG experience in the past 12 months	63.90%	Reduction by at least 15 percentage points within 5 years
Gap between safety training receipt and practical safety knowledge	17.3 percentage points (58.9% trained vs 41.6% knew how to respond)	Closed to within 5 percentage points within 3 years
Share of affected women who report incidents to platforms	32%	Raised to at least 50% with platforms publishing response data quarterly
Share of affected women who access psychosocial care or peer support	Not directly measured (about 27% disclose to friends and family)	At least 30% of affected women accessing some form of support service
Number of Nigerian universities embedding safety units inside existing curricula	Not yet tracked	At least 20 institutions within 3 years
Number of platforms publishing Nigeria-specific TFVAWG response data (general and AI-enabled)	Not yet tracked	All major platforms operating in Nigeria within 2 years
Share of platform takedown requests for AI-generated harmful content actioned within 48 hours in Nigeria	Not yet tracked	At least 80% within 48 hours, with quarterly public reporting
AI detection accuracy for Yoruba, Igbo, Hausa and Pidgin English on platforms operating in Nigeria	Not yet tracked	Detection parity with Englishlanguage content within 5 years

Source: Authors' synthesis based on findings. Targets are indicative and should be refined in consultation with stakeholders.

• Stakeholder Action Matrix

The findings in this brief are most useful when different stakeholders see themselves in them and act on the parts within their reach. Government agencies can use the findings to update existing frameworks. NGOs can use them to redesign training and survivor-support programmes. Platform companies can use them to set Nigeria-specific accountability standards. Academic institutions can use them to embed safety content inside subjects' students are already studying. Donors and international organisations can use them to direct funding towards the highest-leverage points.

Table 3 below translates this into a concrete action matrix. The cells lead with imperative verbs to indicate what each stakeholder can do, mapped against three time horizons. The actions cover both general TFVAWG response and the AI-specific implications discussed throughout this brief.

Stakeholder	Immediate action (0 to 6 months)	Medium term (6 to 18 months)	Longer term (beyond 18 months)
Federal Ministry of Women Affairs	Audit existing TFVAWG referral pathways. Publish a directory of survivor services available across the six geopolitical zones.	Fund anonymous peer helplines. Resource psychosocial care in partnership with NGOs working in lower-income states.	Embed TFVAWG indicators into the national genderbased violence monitoring system. Report progress publicly each year.
NITDA	Revise the National Digital Literacy Framework to add safety-specific competencies, legal-rights content and deepfake awareness modules.	Introduce peer-network mapping into baseline assessments for digital literacy programmes. Track indicators for AI-enabled TFVAWG exposure separately.	Build a public dashboard tracking the gap between training receipt and practical safety knowledge. Maintain a separate AI-safety knowledge measure.
Nigerian Communications Commission	Issue licensing guidance requiring platforms to publish TFVAWG response statistics for Nigerian users. Specify deepfake takedown rates as a reported metric.	Establish a transparency standard for platform takedown response times and appeal mechanisms. Cover AI-generated harmful content explicitly.	Coordinate with ECOWAS regulators on a regional platform accountability framework. Include AI-driven harm in the scope.

Stakeholder	Immediate action (0 to 6 months)	Medium term (6 to 18 months)	Longer term (beyond 18 months)
Nigeria Data Protection Commission	Issue operational guidance on the application of the Nigeria Data Protection Act 2023 to non-consensual deepfake imagery cases. Publish clear redress pathways.	Enforce data-handling standards on platforms processing TFVAWG complaints from Nigerian users. Include AI-generated content in enforcement.	Develop a redress framework for AI-generated synthetic content harms. Provide for cross-border enforcement provisions.
Platform companies operating in Nigeria	Publish Nigeria-specific TFVAWG report response times, action rates and appeal processes. Report AI-generated harmful content as a separate line.	Invest in detection algorithms for Yoruba, Igbo, Hausa and Pidgin English. Improve deepfake detection for Nigerian users.	Co-design moderation policies with Nigerian civil society and survivor groups. Build explicit AI-driven harm response into the policies.
NGOs and civil society	Map peer-network risk among current programme beneficiaries. Identify highrisk participants for targeted support.	Run survivor-support groups and peer-education initiatives. Partner with universities for sustained delivery.	Build a national community of practice on TFVAWG response. Convene actors across government, civil society and platforms.
Universities and academic institutions	Embed practical safety units into journalism, social work, computer science and communication studies curricula.	Run student-led peer safety initiatives on campus and through alumni networks.	Contribute to the regional research base on TFVAWG patterns and intervention effectiveness. Publish findings openly.

Source: Authors' synthesis based on findings

Methodological Note: This brief is grounded in rigorous Qualitative Comparative Analysis (QCA). Unlike standard correlational regression, QCA's set-theoretic approach identifies the complex combinations of conditions (necessity and sufficiency) that produce specific outcomes, allowing for nuanced policy prescriptions that address intersectional realities.

About this brief and the institutions behind it

Centre for the Study of the Economies of Africa (CSEA): CSEA is an independent, non-profit research organisation based in Abuja, Nigeria, with a mandate to conduct policy-relevant economic and social research that supports inclusive development across Africa.

Advancement of Equality, Gender and Inclusion Studies (AEGIS): AEGIS is a research centre at the University of Portsmouth, United Kingdom, working on building evidence and research capacity on how to end gender inequality and social injustices and promote inclusiveness and diversity

Gender and Responsive Artificial Intelligence Network (GRAIN): GRAIN is a consortium composed of two think tanks, IPAR (Initiative Prospective Agricole et Rurale) and CSEA (Centre for the Study of the Economy in Africa), and the non-governmental organisation Sunbird AI. By combining policy research, economic analysis, and AI expertise, the consortium examines both the opportunities and challenges associated with AI adoption and generates evidence to inform policies and interventions that support inclusive and sustainable development in Africa.

About this brief. This brief summarises the results from the report of the TFVAWG project titled “**The Urgency of Safer Digital Spaces for Women and Girls in Africa in the Artificial Intelligence (AI) Era:**

Exploring the Role of Education and Digital Literacy as Protective Factors Against Technology-Facilitated Violence Against Women and girls (TFVAWG) in Nigeria.” The full report contains the complete methodology, descriptive tables, calibration anchors, fuzzy truth tables and configurational solutions which underpin the findings discussed here. The full report is available on request from CSEA (Abuja, Nigeria) and AEGIS (University of Portsmouth, United Kingdom). Ethical approval for the study was granted by the University of Portsmouth under reference FHSS 2025-089.

Recommended Citation:

Onyekwere, S. C., Adeniran, A., Bradley, T. (2026). The Digital Literacy Paradox: Understanding Technology-Facilitated Violence Against Women and Girls in Nigeria [Policy Brief]. Centre for the Study of the Economies of Africa (CSEA)