RAPID TFGBV ANALYSIS REPORT

STOP TFGBV: Support to Overcome and Prevent Technology-Facilitated Gender-Based Violence

Funded by UNTF

By: ELiDA Ethiopia
Date: February 2026
Location: Addis Ababa, Ethiopia

Lead . Inspire . Empower

1. Key Findings Summary

The Digital Safety Paradox

While nearly 90% of sampled individuals own smartphones, technical literacy for digital security is almost entirely absent creating a society that is hyper-connected yet fundamentally unprotected.

62.86%	100%	86.43%
Have experienced online abuse	Unaware of cybercrime reporting platforms	Feel community dismisses online violence

The STOP TFGBV study conducted in Mekelle reveals a community in a state of digital crisis. Cyber-harassment and hacking are the most prevalent forms of abuse, affecting 62.86% of the 140 participants indicating that digital violence is not an isolated occurrence but a lived reality for the majority of young people in Mekelle.

Institutional support is currently at zero-baseline: all respondents are unaware of any government websites, NGOs, or specialized counseling centers for reporting cybercrimes. Focus Group Discussions (FGDs) with young women suggest digital spaces are perceived as lawless zones beyond the reach of formal justice. Key Informant Interviews (KIIs) with social workers confirm that 65.71% of survivors remained silent primarily because they were never taught how to seek help.

Furthermore, while 53.57% recognize online abuse as equally damaging as physical violence, 86.43% feel the broader community dismisses such incidents as trivial. The data is clear: unless a human-centered reporting system is established accounting for the 76.43% preference for human-led hotlines survivors will continue to suffer in silence.

2. Scope and Purpose of the TFGBV Analysis

The TFGBV analysis was conducted within the urban and semi-urban context of Mekelle, Tigray. The scope involved a detailed assessment of the digital lives of at-risk communities, focusing primarily on the intersection of technology use and gender-based safety risks. The primary purpose was to establish a rigorous baseline of digital vulnerability against which the success of future protection, awareness, and legal advocacy programs can be measured.

Specific Objectives

- To establish a quantitative baseline for the percentage of individuals experiencing TFGBV and identify specific technical gaps, including lack of Two-Factor Authentication (2FA) and privacy setting management.
- To assess the current status of reporting behaviors and the existence or total absence of institutional support mechanisms, providing a foundation for future digital safety training and referral network mapping.
- To gather evidence-based insights into social perceptions of online violence in Mekelle, ensuring resources are strategically allocated toward the most targeted groups: young women and adolescent girls.

3. Methodology

The analysis utilized a rigorous mixed-methods approach, blending quantitative metrics from the KoboToolbox report with qualitative narratives from Focus Group Discussions (FGDs) and Key Informant Interviews (KIIs). This methodology was designed to triangulate findings, ensuring that statistical data regarding hacking and harassment was supported by the lived experiences of survivors in Mekelle.

3.1 Study Design

The study employed a descriptive, cross-sectional design intended to capture a snapshot of digital safety at the project's onset. The quantitative component defined the scale of need such as the 62.86% abuse rate while the qualitative component explored the underlying reasons behind current behaviors, including social stigma preventing survivors from reporting and widespread legal apathy regarding digital crimes.

3.2 Sampling and Sample Size

The sample size was determined using the Kish Leslie formula, a standard methodology for descriptive studies where the goal is to estimate a population proportion with precision. The parameters were set as follows:

Sampling Parameters
Confidence Level (Z): 1.96 (95% confidence)
Estimated Prevalence (P): 0.1 (10%) conservative to maximize sensitivity to TFGBV indicators
Margin of Error (d): 0.05 (5%)
Required Sample Size (n): 140 individuals
Gender Weighting: 90% female, reflecting the primary population at risk

This sample size provides the necessary statistical power to generalize findings across Mekelle's diverse demographic layers while remaining resource-efficient.

3.3 Quantitative Methods

The quantitative phase employed a multistage sampling design to ensure that the 140 participants were distributed across the varied socioeconomic environments of Mekelle. The primary mechanism was Systematic Random Sampling, operationalized through the Random Walk method. Enumerators used central landmarks as starting points and applied a bottle-spin or predetermined directional rule to establish a travel path, selecting every Nth household based on local density.

Within each selected household, Simple Random Sampling was applied to select the final respondent where multiple eligible residents existed. This dual-layer randomness guaranteed every eligible resident had an equal probability of participation.

3.4 Qualitative Methods

The qualitative phase utilized Stratified Purposive Sampling, focusing on information-rich cases to explore the contextual dynamics of TFGBV. The study population was divided into three strata: young women, youth leaders, and IT specialists. This stratification produced six FGDs and four KIIs, with FGDs structured as homogenous groups to foster safe dialogue on sensitive topics.

3.5 Data Collection Tools

The quantitative phase was powered by KoboToolbox, which facilitated real-time data entry, geographical tagging to verify random walk distribution, and reduced manual entry errors. The qualitative phase used semi-structured interview and discussion guides, allowing facilitators to balance consistency with the flexibility needed for sensitive topics.

3.6 Ethical Considerations

Ethical integrity was the cornerstone of the process. All respondents provided informed verbal or written consent after a full briefing on the study's sensitive nature. Given the potential for re-traumatization when discussing online violence, strict confidentiality protocols were enforced. The team adhered to "Do No Harm" principles, ensuring the data collection process was respectful, culturally appropriate, and did not create new safety risks for survivors.

3.7 Data Analysis

Quantitative data from KoboToolbox was processed to generate descriptive statistics, including frequencies and percentages for all Key Performance Indicators (KPIs). Qualitative data underwent thematic content analysis, where recurring narratives from FGDs were coded and used to contextualize and humanize the statistical findings.

3.8 Limitations

Self-reported data on digital habits may be influenced by social desirability bias. The legal hopelessness prevalent in Mekelle may have shaped responses regarding the need for stricter laws. Additionally, as a cross-sectional study, the snapshot nature of the data may not fully capture the rapidly evolving social media landscape. Nonetheless, these findings remain a reliable and essential foundation for the project's monitoring and evaluation framework.

4. Respondent Profile

90%	62.86%	6.43%
Female respondents (126 individuals)	Aged 25–34 years	Persons with disabilities

The sample is intentionally gender-weighted, with 90% (126 individuals) female and 10% (14) male, reflecting the community's own identification of young women as the primary group at risk (47.14%). The age distribution is predominantly young: 62.86% fall into the 25–34 age range, and 19.29% represent the 15–24 youth segment largely digital natives who rely on these platforms for social and professional engagement.

Qualitative insights from FGDs reveal that women in the 25–34 age group are particularly targeted because they are more likely to use digital tools for networking, entrepreneurship, and public social interaction providing more exposure to potential abusers. Persons with disabilities (6.43%) face even higher barriers to accessing help, as noted by KII participants.

All respondents are situated within Mekelle, ensuring findings are contextually specific to the region. The 100% consent rate among participants underscores a profound community desire to engage with this topic signaling that the silence surrounding TFGBV is not a choice made by victims, but a result of a lack of safe outlets for disclosure.

5. Access to Digital Devices & Internet

> **Key Insight: The Digital Divide Has Shifted**
> *In Mekelle, the divide is no longer about access to hardware it is about safety. Most users possess the devices but lack the security knowledge to use them safely.*

In Mekelle, the smartphone has transitioned from a luxury to an essential utility. 87.14% of respondents personally own a smartphone, indicating widespread individual and private access to the digital world, with only 10.71% relying on shared devices.

Internet connectivity is dominated by mobile data (66.43%), with 25.71% using WiFi. FGDs indicate that mobile data users are often "online on the go," making them more susceptible to real-time tracking and impulsive digital interactions that can lead to harassment. Only 7.14% use computers or tablets, meaning the majority of TFGBV is concentrated in the mobile app ecosystem.

The private nature of smartphone use verified by 85% of respondents who report never being monitored by household members creates a double-edged reality: it provides privacy from family, but leaves the user isolated when a digital attack occurs.

6. Social Media Usage

46.43%	~50%	36.43%
Use TikTok most frequently	Spend 2–3 hours/day on social media	Share location always or sometimes

Social media usage in Mekelle is characterized by high intensity and a strong preference for video-centric platforms. TikTok has rapidly emerged as the dominant platform (46.43%), followed by Telegram at 24.29%. The primary motivation for engagement is entertainment (47.86%), which shapes the nature of the abuse encountered.

FGD participants noted that the shift toward TikTok has moved harassment from text-based insults to more damaging visual abuse including doctored videos and public shaming in comment sections. While 62.14% report not sharing their location, a combined 36.43% do so always or sometimes. In a localized city like Mekelle, this data can easily be exploited for physical stalking.

Because usage is primarily entertainment-led, users are typically in a relaxed state of mind when online, making them less vigilant against social engineering and phishing attempts the same mechanisms contributing to the 41.43% hacking rate reported in the survey.

7. Online Safety & Privacy

> **Critical Risk Finding**

> 75.71% of respondents do not use Two-Factor Authentication (2FA) not by choice, but because they do not know how to set it up. This technical gap is a primary driver of the 41.43% account hacking rate.

The security posture of users in Mekelle is dangerously fragile. Beyond the 2FA gap, privacy settings are treated as static 46.43% have never adjusted them, and 34.29% did so only once. While 93.57% are cautious about not sharing passwords with family, this internal caution does nothing to prevent external technical breaches.

FGDs revealed a widespread belief that standard passwords provide sufficient security, with users unaware of the sophisticated tools used by hackers today. KIIs with local law enforcement confirmed they are frequently overwhelmed by complaints of account takeovers but lack the technical capacity to provide assistance.

This highlights a critical disconnect: users are protecting their accounts from their immediate social circles while leaving them open to external attackers effectively navigating a high-risk digital environment without any defensive infrastructure.

8. Vulnerability Analysis and Risk Factors

Vulnerability to TFGBV in Mekelle is not random it is structural and gendered. The primary risk factors combine technical vulnerability (lack of 2FA, unmanaged privacy settings) with social isolation and community normalization of digital harm.

Primary Forms of Abuse

- Cyber-harassment: 67.86% of abuse cases
- Account hacking: 41.43% of abuse cases
- Image-based abuse via WhatsApp and Telegram: 34.29% where private messages can be screenshotted and used for extortion

Structural Risk Factors

FGDs with survivors reveal that risk is compounded by the community's dismissive attitude toward digital harm. The 86.43% who feel online violence is not taken seriously creates a secondary trauma, where victims feel they have no right to be upset because the abuse happened "only online." This environment of impunity allows perpetrators to act with confidence, knowing that institutional and social barriers will prevent survivors from seeking support.

9. Awareness, Attitude & Perception of TFGBV

53.57%	93.57%	95.71%
Recognize online abuse as serious as physical violence	Unaware non-consensual image sharing is a crime	Believe stricter laws are not needed

There is a profound disconnect in Mekelle between the recognition of harm and the understanding of digital rights. While 53.57% correctly perceive online abuse as equally harmful as physical violence, 93.57% are unaware that sharing someone's private photos without consent constitutes a form of violence. The community feels the pain of TFGBV but lacks the vocabulary and legal framework to define it as a crime.

FGD participants frequently reported a sense of "digital shame" assuming they must have done something to attract an abuser, even though 77.14% logically disagree with victim-blaming. KIIs with legal advocates point to a pervasive "legal hopelessness": because users have never seen a perpetrator punished, they cannot imagine a protective system, and thus 95.71% see no need for stricter laws. The digital world is perceived as a lawless frontier where the only perceived defense is to withdraw entirely.

10. Awareness & Knowledge of Online Reporting Mechanisms

100% of respondents are unaware of any official government or police platforms for reporting cybercrimes.

97.86% do not know where to find Help or Safety centers within the apps they use daily.

The mechanisms for seeking justice in Mekelle are currently either non-existent or entirely unknown to the population. While 53.57% know how to block a user, nearly half lack even this most basic defensive skill.

FGDs describe a community that relies on informal reporting telling friends (26.43%) or family (15%) rather than seeking professional or institutional help. KIIs with tech activists indicate that existing platform-based reporting tools are too complex and not localized for the Tigrinya-speaking community, resulting in learned helplessness where 65.71% of survivors do not report because they "don't know how."

Critically, 70% of respondents stated they would be "much more likely" to report if an anonymous, culturally sensitive reporting tool were available demonstrating that the absence of reporting is not a sign of a low incidence of harm, but of a failed reporting infrastructure.

11. Access to TFGBV Services & Referral

34.29%	33.57%	25%
Need financial support	Need psychological counseling	Want legal assistance

Service provision for TFGBV in Mekelle is at a complete standstill. All 140 respondents are unaware of any local NGOs, helplines, safe spaces, or counseling services for digital abuse. Despite this total absence of supply, the demand for services is high and specific.

FGDs revealed that TFGBV often carries real-world economic impacts survivors losing employment or business reputations explaining the high need for financial aid. KIIs with healthcare providers confirmed that while staff are trained for physical GBV, they are unprepared to manage the specific trauma of online stalking or non-consensual image sharing.

The community's overwhelming preference (76.43%) for a human-led hotline is particularly telling: survivors do not want to interact with an algorithm they want to speak with a person who understands their culture, their language, and the specific digital landscape of Mekelle.

12. Major Challenges Facing TFGBV Awareness, Reporting, and Access to Services

Challenge 1: The Technical Literacy Gap and 2FA Neglect

While smartphone access is nearly universal at 87.14%, a staggering 75.71% of respondents do not use Two-Factor Authentication simply because they do not know how to set it up. Privacy settings remain unmanaged by 46.43% of users who have never adjusted them. This knowledge gap creates a cycle where users are aware of threats but unaware of solutions, leaving digital abuse to feel inevitable rather than preventable.

Challenge 2: Normalization and the Culture of Social Dismissal

86.43% of respondents feel their community does not take online violence seriously, often dismissing it as "just the internet." This cultural perception creates a validation gap where survivors feel their trauma is illegitimate because it lacks a physical manifestation. FGDs

highlighted that survivors are frequently advised to simply "turn off the phone" trivializing harm that 53.57% correctly identify as psychologically equivalent to physical violence.

Challenge 3: Legal Hopelessness and Rights Illiteracy

A critical 93.57% of participants are unaware that non-consensual image sharing is a criminal act. This rights illiteracy means many survivors do not realize they have been victims of a punishable offense. The belief that the internet is a lawless frontier where 95.71% see no point in stricter laws leaves perpetrators operating with total impunity in Mekelle's digital landscape.

Challenge 4: The Institutional Reporting Vacuum

All 100% of respondents are unaware of any official government or police website for reporting cybercrimes. This institutional invisibility is the primary reason 65.71% of survivors who stayed silent did so because they "didn't know how" to report. Official reporting currently stands at a negligible 1.43%, while 97.86% remain unaware of in-app safety resources.

Challenge 5: Lack of Specialized TFGBV Support Services

100% of participants are unaware of any local NGOs, helplines, or clinics offering support specifically for digital abuse. While survivors identified needs for financial support (34.29%) and psychological counseling (33.57%), the current health and social service sectors are not equipped to handle the nuances of TFGBV, leaving even resilient survivors with nowhere to turn.

Challenge 6: Fear of Stigma and the Digital Shame Barrier

Despite 77.14% logically disagreeing with victim-blaming, FGDs revealed that "digital shame" remains a powerful deterrent. Survivors fear that if they report especially incidents involving hacked accounts or shared images their families and peers will scrutinize their online behavior rather than the perpetrator's crime. This is why 70% of respondents would only report via an anonymous tool. The current reporting landscape demands a level of public exposure that many are unwilling to risk in Mekelle's conservative social context.

13. Recommendations & Stakeholder Mapping

The following eight recommendations are grounded directly in the study's findings. Each is paired with the key stakeholders responsible for implementation, ensuring that recommendations are actionable and aligned with existing community infrastructure.

1

Launch Targeted Social Media Safety Videos

Since 85.71% of the community identifies social media videos as their preferred learning tool, a campaign must be launched on TikTok and Telegram. Videos should be produced in Tigrinya, feature trusted local influencers, and focus on Digital Rights 101 explaining that non-consensual image sharing is a crime and demonstrating how to use platform reporting tools. This brings education directly into the spaces where users already spend 2–7 hours daily.

Stakeholders: *Tigray Youth Association, Mekelle University (ICT Department), local influencers, Women Lead CSOs including ELiDA*

2

Establish Hands-On Technical Safety Workshops

To directly address the 75.71% who cannot set up 2FA, "Digital Safety Clinics" should be held at community centers and TVET colleges. These practical sessions should have participants bring their own phones and receive guided, step-by-step assistance in securing accounts, adjusting privacy settings, and identifying phishing attempts directly targeting the technical vulnerability driving the 41.43% hacking rate.

Stakeholders: *Local TVET colleges, IT student groups, community-based organizations (CBOs)*

3

Establish a Human-Led Hotline

Addressing the 76.43% preference for human interaction, a dedicated hotline must be established. It should be staffed by counselors trained in both psychological first aid and digital safety, providing a one-stop-shop where survivors receive emotional support and are referred to legal or technical experts for content removal and legal action.

Stakeholders: *Regional Bureau of Women Affairs, Ethio Telecom, local mental health NGOs*

4

Develop an Anonymous Reporting Portal

70% of users want an anonymous way to report digital abuse. A simple, localized web portal or Telegram bot should be created where users can upload evidence and receive immediate technical advice without fear of social stigma. The aggregated data can then be used to track trends and build the evidentiary base needed for advocacy and policy change.

Stakeholders: *INSA (Information Network Security Administration), local tech startups*

5

Community and Religious Leader Sensitization

To shift the 86.43% dismissal culture, sensitization programs must target religious leaders and Kebele administrators. By educating community leaders on the psychological and

economic harm of TFGBV, they can begin validating survivors' experiences from community platforms transforming the culture from one of dismissal to one of support.

Stakeholders: *Religious Council of Tigray, Kebele administrators*

6

Integrate Digital Trauma into Clinical Care

Mekelle's health infrastructure must formally recognize digital violence. With 33.57% of survivors requiring counseling, training must be provided to existing GBV clinic staff on how to treat the specific trauma of online harassment and stalking turning currently non-existent safe spaces (100% unaware) into a tangible reality.

Stakeholders: *Mekelle Health Bureau, Ayder Referral Hospital*

7

Legal Awareness Campaigns

With 93.57% unaware that non-consensual image sharing is a crime, a legal literacy campaign is urgently needed. Using radio and community posters, the campaign should explain existing cybercrime laws and the steps required to file a police report bridging the legal hopelessness experienced by 95.71% of the population.

Stakeholders: *Mekelle Justice Bureau, local lawyers' associations*

8

School-Based Digital Literacy Integration

To protect the next generation (the 15–24 age group), digital safety must be integrated into secondary school and university orientation curricula. Teaching young people early about consent, digital footprints, and security protocols will build a long-term culture of digital resilience in Mekelle.

Stakeholders: *Regional Education Bureau, Parent-Teacher Associations*

Lead . Inspire . Empower