Reclaiming Safe Space: Digital Violence, The Threat to Libyan Women, and the Urgent Demand for Protection

Digital violence against women and girls in Libya is no longer an isolated phenomenon; it is a critical, systemic threat that weaponizes technology to perpetuate and amplify Gender-Based Violence (GBV). This abuse—ranging from cyberstalking and non-consensual image sharing to targeted defamation—has severe consequences far beyond the screen.

In a context marked by institutional fragility and complex security challenges, the digital realm has become a powerful tool for enforcing patriarchal control, silencing female activists, journalists, and public figures. Crucially, in Libya, digital abuse acts as a precursor to severe, real-world human rights violations, including physical violence, arbitrary detention, and enforced disappearance. The current danger is significantly exacerbated by the failure of Libyan authorities to establish protective legal frameworks and, in some cases, the exploitation of digital communication by institutional and non-state actors to target women.

Within the crucial framework of the 16 Days of Activism against Gender-Based Violence of 2025 (November 25 – December 10), the World Organisation Against Torture (OMCT) and the Libyan Anti-torture Network (LAN)'s goal is to mobilize a united response to reclaim and secure the digital spaces essential for women's safety, participation, and expression.

I. Defining the Crisis

Digital Violence as Gender-Based Violence (GBV): In the Libyan context, acts of gender-based digital violence are pervasive and include doxing (publishing private personal information to incite offline harassment), cyberstalking and harassment through repeated, targeted threats, non-consensual sharing of intimate images (often referred to as 'revenge porn'), and systemic campaigns of hate speech and defamation designed to discredit women based on their gender or public role.

Institutional Responsibility, Data Gaps, and Vulnerability: The expansion of social media, combined with the lack of centralized state control, porous security, and a challenging environment for human rights defenders, creates a heightened risk. Digital tools are frequently exploited by state, non-state actors, and individuals to control, intimidate, and punish women who defy traditional gender roles or engage in public discourse. This danger is compounded by the proliferation of racist and anti-migrant rhetoric across platforms, leaving women migrants and asylum-seekers disproportionately vulnerable to targeted abuse, exploitation, and state-sanctioned violence.

Despite the visible severity, significant data gaps remain due to critically low reporting rates and the absence of a unified national mechanism to compile accurate information, leading to a distorted understanding of the true scale of digital violence in Libya.

Libyan authorities bear direct responsibility for the data and security gaps, both through the inadequacy of existing laws and the failure to hold perpetrators accountable. Furthermore, the use of digital content as a pretext for arbitrary arrest and detention fundamentally breaches the state's obligation to protect its citizens.

II. The Consequences in the Libyan Context

Psychological and Social Impact: Digital violence inflicts profound and systemic harm, extending far beyond the online sphere. Evidence documented by LAN members confirms the consequences include severe psychological trauma, manifesting as acute anxiety, sleep disturbances, and a pervasive sense of fear and loss of control over personal privacy. These gendered abuses are strategically deployed to dismantle victims' reputations, enforce social isolation, and result in the loss of professional or educational opportunities.

LAN has obtained valid evidence proving that several female survivors who were subjected to torture in detention as a result of digital violence that translated into the real world are currently battling catastrophic social consequences. Not only have these survivors had to abandon activism or been fired from their jobs, but many have also been jailed at home by their families, been forced to divorce, and many mothers have lost custody of their children. The psychological and social harms of such violence are extensive, impacting the victims' families and children in many public spheres, thereby eroding their fundamental right to public participation and safety.

From Digital Abuse to Real-World Violence: Beyond the psychological toll, digital violence is intentionally deployed as a political weapon to silence female activists, journalists, and human rights defenders, effectively shrinking the space for women to contribute to Libya's stabilization. This online hostility routinely escalates into severe real-world human rights violations, where doxing and targeted threats act as direct precursors to financial abuses, sexual exploitation, arbitrary detention, and "unofficial" summons based on online posts. In its most extreme form, the systematic digital targeting of women in Libya facilitates enforced disappearances, as online content is weaponized by state and non-state actors to identify, isolate, and abduct victims, cementing the reality that online visibility has become a critical security liability.

Case Study: The Targeting of Wedad Al-Shariqi: The case of Wedad Al-Shariqi perfectly illustrates this harrowing trajectory. Her ordeal began with systematic digital targeting, including repeated threats and hacking attempts, before escalating into a grave institutional betrayal where the Public Prosecution exposed her sensitive data—specifically her mother's phone number—to a militia member who used it to facilitate her kidnapping. Despite the severity of these death threats and extortion, her legal complaint was classified as a minor misdemeanor, highlighting the judicial system's failure to recognize digital violence as a lethal threat. This recent violence followed years of harassment dating back to 2016, when malicious photo leaks were used in an attempt to expel her from university, demonstrating how digital tools are persistently used to punish women for their presence in public spaces.

III. Legal and Platform Accountability Gaps

Legal Vacuum in Libya: Existing Libyan laws were not designed to address the complex, transnational nature of digital violence, resulting in a significant legal vacuum. The implementation of the Anti-Cybercrime Law No. 5 of 2022 since 2023 has also been a critical concern: rather than protecting victims, the law is being actively used to restrict women's freedom of expression and justify arbitrary arrests based on vague accusations of "violating public morals" online. Critically, the Cybercrime Law remains inadequate as it primarily focuses on cyber-security or general defamation and fails to explicitly criminalize the gendered nature of violations such as non-consensual image sharing or doxing when directed at women. While a draft law on combating violence against women and girls exists and

addresses specifically online violence, its failure to be ratified leaves victims unprotected by comprehensive GBV-specific legislation.

This legislative gap ensures that authorities frequently exploit existing laws to justify the arrest and prosecution of the victims of digital violence, rather than the perpetrators. The situation is compounded by the fact that while a dedicated reporting mechanism for violence against women and girls was established by the western government in 2023—and has prompted a similar initiative in the East—these mechanisms face significant limitations due to social stigma, fear of reporting, and a lack of public trust. This highlights the urgent need to fully institutionalize and expand these channels to guarantee victims' safety and confidentiality.

Platform Failure & Tech Company Accountability: Major international social media platforms (such as Meta-owned Facebook and WhatsApp) are not above the law and must be held accountable under both national and international human rights frameworks for the harms facilitated on their networks. These companies have demonstrated key failures to adequately safeguard their Libyan users. These failures include slow, inconsistent, and often non-existent responses to reports of abuse due to inadequate Arabic moderation capacity.

Furthermore, corporate governance and shifting priorities often result in systemic biases that disproportionately affect women and marginalized groups, leading to the inconsistent application of safety policies. This lack of accountability is exacerbated by a failure to establish specialized protocols to quickly verify and protect high-risk users, such as women human rights defenders, who are known targets of sophisticated, sustained threats, effectively allowing impunity to flourish.

IV. Recommendations

We call on all actors to mobilize immediately to reclaim safe space for women in Libya.

To Libyan Authorities:

1. Legislative Reform: Urgently amend the Cybercrime Law and Penal Code to explicitly criminalize digital violence (doxing, extortion, harassment) as independent violations rather than minor misdemeanors and ratify the draft Law on Combating Violence Against Women and Girls.

2. Ensure Accountability: Investigate and prosecute state and non-state actors who weaponize digital data to facilitate arbitrary detention or physical harm of women, accounting for intersecting vulnerabilities, including those based on migration status or race.

3. Strengthen and Expand Reporting Mechanisms: Strengthen the reporting mechanism for violence against women and girls established in the West. This mechanism must be expanded into a secure, national platform to compile accurate data on digital violence, addressing existing limitations such as social stigma and public mistrust, and ensuring all security and judicial staff receive specialized training on victim-centered referral pathways.

4. Digital Literacy and Education: Integrate effective digital awareness programs into schools, institutes, and universities. This includes introducing digital security concepts into the core curricula and providing mandatory explanations and specialized courses on the risks associated with electronic extortion and cyberbullying.

To Tech Companies and Social Media Platforms:

1. Culturally Competent Monitoring & Moderation: Strengthen advanced digital monitoring to document systematic repression and the use of sophisticated tools like deepfakes. Significantly increase human moderation capacity in Arabic, ensuring cultural competency, gender sensitivity, and accountability for systemic biases that disproportionately affect women and marginalized users.

2. International Human Rights Due Diligence: Establish verifiable human rights due diligence processes in line with the UN Guiding Principles on Business and Human Rights (UNGPs) and international human rights frameworks, particularly for high-risk regions like Libya, and commit to addressing harm resulting from platform failures and inconsistent policy application.

Published by:

World Organisation Against Torture (OMCT) & Libyan Anti-torture Network (LAN)