

## **Kenya's laws fail to protect women from AI-enabled abuse**

**By Faith Muiruri**

Artificial intelligence (AI) is transforming how Kenyans communicate, learn, work and participate in public life. But the rapid spread of AI tools is also opening new avenues for gender-based violence that the country's legal and institutional systems are not yet prepared for.

A new analysis by the Community Advocacy and Awareness Trust (CRAWN Trust) says Kenya faces a widening regulatory vacuum as deepfakes, voice cloning, synthetic intimate images, automated harassment and AI-generated disinformation become easier to produce and distribute.

The study, funded by the African Women's Development Fund, describes technology-facilitated gender-based violence as a rapidly evolving threat that affects not only personal safety, but also elections, education, financial inclusion, and national development.

Among the most urgent risks, is the creation of non-consensual intimate imagery using generative AI. "Such images can be fabricated without any physical encounter between the perpetrator and victim. A photograph posted online may be manipulated into sexually explicit material within minutes and distributed across multiple platforms before the victim even knows it exists," says the report.

The report further notes that the damage is often immediate and difficult to reverse. "Harmful content can be copied, reposted and stored indefinitely."

It refers to this as a "digital tattoo" where a permanent record of abuse, forces survivors to relive the violation whenever the material reappears.

Currently, Kenyan laws do not specifically criminalise the creation of AI-generated non-consensual sexual imagery. The study observes that existing provisions may address some forms of harassment or the distribution of intimate images, but they do not adequately cover synthetic content, voice cloning, or the tools used to create it.

### **Electioneering period**

"This legal uncertainty becomes even more dangerous during an electioneering period," adds the report.

What is worrying is that AI-generated videos, audio and images could be used to impersonate women candidates, spread sexualised rumours, distort their statements or create false evidence.

"With Kenya's high mobile penetration and uneven digital literacy, fabricated content could circulate widely before it is verified."

The report explains how coordinated online campaigns can combine fake accounts, doxing, abusive comments and misleading narratives to damage a candidate's reputation and discourage

her from campaigning. “Such attacks may appear to be ordinary political criticism, but the report argues that many are designed to silence women and exclude them from public participation.”

The risk extends to journalists and activists. “AI-generated audio could be used to falsely attribute statements to a reporter or human rights defender. Synthetic videos could undermine public trust in legitimate investigations. Women who speak about corruption, governance or violence may become targets of coordinated disinformation intended to force them offline.”

### **Artificial Intelligence Bill**

The report raises concerns about the Artificial Intelligence Bill, 2026, currently before the Senate. It describes the Bill as an important starting point, but says it requires substantial amendment before enactment.

The report singles out institutional fragmentation as one of the areas that need further consideration. According to the report, the proposed creation of several new AI oversight bodies alongside existing institutions such as the Office of the Data Protection Commissioner and the Communications Authority, could leave survivors unsure where to report.

“A woman whose likeness has been used in an AI-generated sexual image might have to deal separately with police investigators, data regulators, cybercrime bodies, and online platforms.”

The report recommends that the AI Commissioner, if established, should coordinate with existing institutions rather than create parallel and competing systems. It calls for a single, integrated complaint pathway for AI-related gender-based violence.

The Bill should also classify systems designed to generate non-consensual sexual imagery or impersonate real people for harmful purposes as prohibited-risk applications. It should include specific protections for children, electoral safeguards and mandatory testing against cyber threats such as model poisoning and prompt injection.

For children, technology-facilitated abuse often begins in schools, peer messaging groups, online classrooms and social media. “Girls may face cyberbullying, grooming and the circulation of intimate images, while boys may be exposed to online communities that normalise misogyny and entitlement.”

Of concerns to children rights advocates is that the rollout of AI-enabled learning tools under the Competency Based Curriculum has also raised questions about children’s data. The report says parents may not have sufficient information about how behavioural, biometric, or learning data is collected, processed and used.

### **Children Act**

It recommends amending the Children Act to recognise technology-facilitated child abuse explicitly. “Digital platforms used by children should have age-appropriate safeguards, accessible reporting tools and parental consent mechanisms.”

“The Ministry of Education should oversee AI systems used in schools in coordination with data protection and cybercrime authorities.”

In addition to children, the report notes that women are experiencing serious economic digital abuse. Control over M-Pesa credentials, forced disclosure of passwords, monitoring of transactions and unauthorized digital loans are being can be used to trap women in abusive relationships. “Yet financial regulations do not clearly recognise digital financial coercion as gender-based violence.”

The report calls on the Central Bank of Kenya to establish reporting and remedy pathways for technology-enabled economic abuse. Mobile money and digital finance providers should develop safety triggers for suspicious transaction patterns and mechanisms to help survivors restore control over their accounts.

### **Digital protection orders**

This should be treated with urgency since protection from service providers remains an area of concern. Google transparency report, for instance, shows that approximately 62 per cent of Kenyan government content-removal requests were rejected during the first half of 2025. For survivors of intimate-image abuse, delays can mean that content is viewed and copied thousands of times.

To ensure compliance by such companies, the proposed reforms include requiring platforms to act within 24 hours to remove offending content, stronger penalties for non-compliance, and mandatory local content moderation and transparency reports on complaints. The study recommends online platforms to develop moderation capacity in Swahili and other local contexts.

Other recommendations in the report include: Development of county-level forensic capacity and specialized prosecution units; creation of precise, proportionate laws that distinguish lawful speech from threats, harassment, intimidation, sexual exploitation and coordinated digital violence; and ratification of the International Labour Organization’s Convention 190, which recognises violence and harassment in technology-enabled workplaces.

Kenya’s AI future is being shaped today. If safeguards are delayed, the country may find itself responding to harms that have already spread beyond control. If reform is pursued urgently and coherently, technology can remain a tool of innovation rather than becoming an instrument of intimidation.