UNIVERSITY of the WESTERN CAPE

FACULTY of LAW

Journal of Anti-Corruption Law

Combatting Economic Crime and Trafficking: Economic & Cybercrimes Conference VIII

TOPIC: Cyber-Enabled Child Trafficking in Africa: Risks, Legal Gaps and Towards a Survivor-Centred Cyber-Justice Model

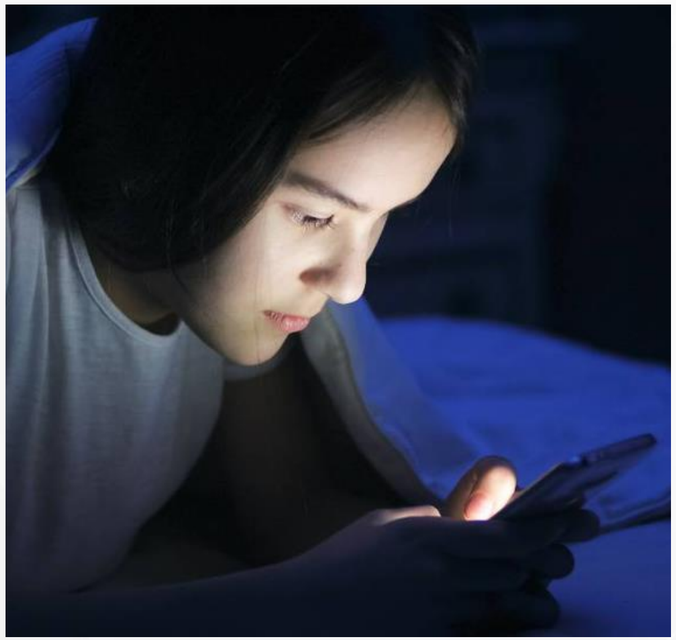
PRESENTED BY **PAUL MUKIIBI**

DATE: September 04, 2025

TIME: 8am to 3pm

SCHOOL OF PUBLIC HEALTH (UWC)

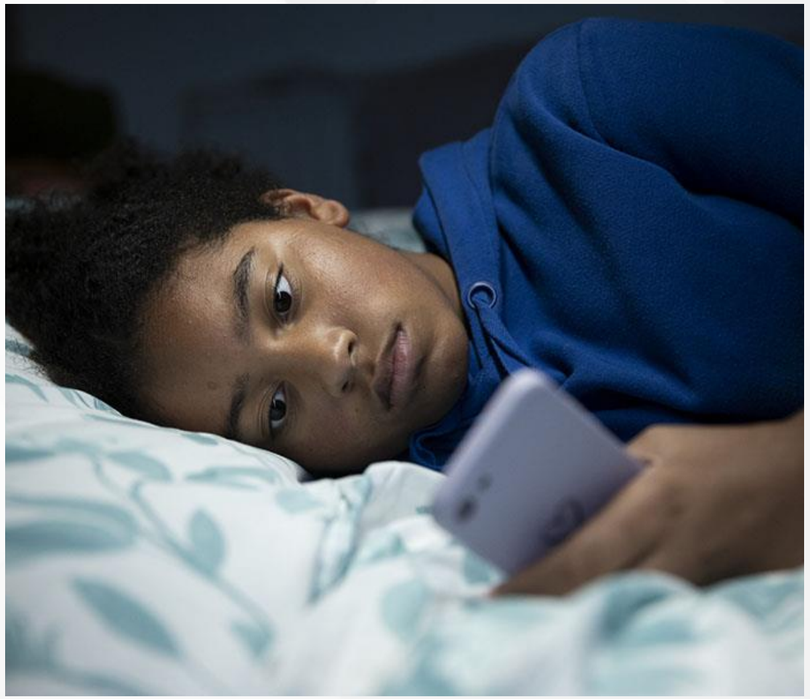
Introduction



Africa's rapid digital expansion is reshaping children's lives. According to the **United Nations Office on Drugs and Crime**, by **2022**, **43 percent** of Sub-Saharan Africa's population was online, and **42 percent** were under **14 years old**. While children benefit from connectivity, traffickers exploit social media, gaming platforms, and messaging apps for grooming, sextortion, live-streamed abuse, and trafficking.

Cheap smartphones and data bundles extend these risks even into rural areas. Exploitation thrives where poverty, conflict, discrimination, and family breakdown create vulnerabilities.

The **African Child Policy Forum** notes that unidentified victims of online child sexual exploitation are often very young - more than **60 %** were infants or toddlers, and **65** % were girls.



How Predators Operate

Predators use two main strategies, described by the **United Nations Office on Drugs and Crime** as ***hunting*** (actively seeking children) and ***fishing*** (posting deceptive offers or messages and waiting for replies). They lure victims with promises of work, education, or romance, later coercing them into sexual exploitation or forced criminality. Exploitation is enabled by weak legislation, poor reporting systems, and social stigma. Offenders also exploit digital anonymity through social media, dating apps, and live-streaming platforms, making it easier to evade detection and expand their reach across borders

Scale and patterns of abuse

The **Disrupting Harm Project** (ECPAT, INTERPOL & UNICEF) revealed that in **2020**, millions of children in **13 African countries** were subjected to online sexual exploitation and abuse. Prevalence rates ranged from **1 to 20 percent**. Yet only **3 percent** of victims contacted police or helplines, and almost **one in three children** did not disclose the abuse to anyone. Many victims reported not knowing where to seek help or fearing stigma and retaliation. The study also found that **Facebook and Messenger** accounted for over **90 percent** of reported cases in some countries.

Studies by **Child Fund International** and the **African Child Policy Forum** similarly reveal high exposure to online risks.

- Across **Ethiopia, Mozambique and South Africa**, around **one fifth of children aged 12-17** received unsolicited requests to talk about sex and a significant portion went on to meet the person face to face.
- Up to one third of children in **Ethiopia and Mozambique** shared personal information with strangers, and **19 % of 9 to 17 year olds** in **South Africa** and **21 % of 15 to 17 year olds** in **Uganda** received unwanted sexual requests.

- In **Kenya and Mozambique**, up to **13 %** of adolescents were threatened or blackmailed to engage in sexual activities, and over one quarter of teenagers in Mozambique and one third in South Africa met a stranger in person after online contact.
- Such findings confirm that digital grooming frequently culminates in physical exploitation.

Categories of Perpetrators

- **Traders** – collect and distribute child sexual abuse material.
- **Networkers** – build communities of offenders.
- **Groomers** – establish online contact with children.
- **Travellers** – arrange physical meetings.
- **Traffickers** – recruit, transport, or harbour children.

Technology enables offenders to move between these roles, supported by encrypted apps, the dark web, and cryptocurrencies.

COVID-19 Impact

The pandemic amplified risks. Lockdowns and school closures pushed children online, while families faced financial strain. Traffickers shifted to fully digital grooming, using gaming platforms, dating apps, and fake profiles. At the same time, in-person support services shut down or moved online, leaving children in abusive homes with fewer avenues for protection. The **U.S. Trafficking in Persons Report 2024** documents sharp increases in online commercial sexual exploitation and child sexual abuse material during the pandemic, as traffickers refined their digital schemes to operate without ever meeting victims in person

Consequences for Victims

The harms are lifelong. Victims report trauma, shame, social isolation, and mistrust of digital spaces. According to the **Disrupting Harm study**, online exploitation is strongly associated with higher risks of self-harm and suicidal ideation. Social attitudes worsen the problem: in **Ethiopia, 73 percent of children and 84 percent of caregivers** said victims who shared intimate images were at fault if those images were leaked. Such victim-blaming deters reporting and deepens stigma.

International Legal Frameworks

- **Protocol to Prevent, Suppress and Punish Trafficking in Persons or Palermo Protocol**: defines trafficking; Article 9 requires prevention programmes; Article 10 mandates information exchange and training; Article 11 strengthens border controls.
- **Convention on the Rights of the Child (1989)**: Article 34 requires protection from sexual exploitation; Article 35 obliges prevention of abduction, sale, or trafficking.

- **The Optional Protocol on the sale of children, child prostitution and child pornography (2000)**: prohibits sale of children, child prostitution, child pornography; mandates extraterritorial jurisdiction and child-friendly procedures.
- **The International Labour Organisation's Worst Forms of Child Labour Convention (No. 182)(1999)**: prohibits the worst forms of child labour, including trafficking.
- **UN Committee on the Rights of the Child adopted General comment No. 25 (2021)**: applies all Convention on the Rights of the Child rights to the digital environment

African Legal Frameworks

- **African Charter on the Rights and Welfare of the Child (1990):** Article 27 protects children from sexual exploitation; Article 29 requires states to prevent abduction, sale, or trafficking.
- **Declaration on ending and preventing online child sexual exploitation (2019)**: urged states to criminalise online grooming and strengthen cooperation.
- **Convention on Cyber Security and Personal Data Protection** or the **Malabo Convention (2014)**: Article 25 affirms cybercrime legislation must respect rights such as privacy and fair trial.

- **AU Child Online Safety and Empowerment Policy (2024)**: The policy assesses opportunities and risks related to digital access and identifies cross cutting issues, such as data protection, gender and disability inclusion, and multilingual education, before setting ten strategic goals including aligning laws with global standards, building survivor services, enhancing personal data protection, and ensuring corporate responsibility.

Legal Gaps

- The **UN Conference on Trade and Development** reports that around **72 % of African countries** have cybercrime legislation, and by **2023** roughly **33-36 countries** had adopted data protection laws

- **INTERPOL's 2025 Africa Cyberthreat Assessment** reports that **75 % of African countries** say their legal frameworks and prosecution capacity need improvement and **95 %** cite inadequate training, resource constraints and a lack of specialised tools.

- Only **30 %** of countries have an incident reporting system, **29 %** maintain a digital evidence repository and 19 % host a cyber threat intelligence database. More than **86 %** of countries acknowledge that international cooperation capacity must be enhanced due to slow, formal processes and limited access to foreign hosted data, while **89 %** report significant barriers to working with the private sector because engagement channels are unclear and institutions are unprepared. These statistics illustrate a continent wide mismatch between the sophistication of cyber criminal networks and the resources available to pursue them

- Existing legislation often fails to explicitly criminalise online grooming, sextortion or possession of child sexual abuse material, forcing prosecutors to rely on general offences that may not capture the nuances of digital exploitation. Harmonising and updating these legal frameworks, while ensuring they respect fundamental rights, is crucial for effective prosecution.

- Enforcement remains weak due to scarce forensic resources and fragmented legal definitions that frustrate cross-border investigations

Challenges in prosecution and law enforcement

Cyber-enabled child trafficking is difficult to prosecute because crimes cross borders, offenders hide behind digital tools, victims are often reluctant to testify, and laws lag behind technology, according to UNODC and the U.S. Trafficking in Persons Report, which both warn that enforcement has not kept pace with online realities.

- **Jurisdiction and cross-border evidence:** Most electronic evidence is stored overseas, forcing African investigators to rely on the outdated Mutual Legal Assistance Treaty (MLAT) system, which is slow and ineffective; in 2019, major platforms received only **63 requests** from the entire continent per UNODC, and the UN Conference on Trade and Development reports that **72 % of African countries** have cybercrime legislation, and by 2023 roughly **33-36 countries** had adopted data protection laws, leaving traffickers free to exploit these gaps.
- **Encryption, anonymity and evolving technology:** Traffickers use encryption, VPNs, dark web markets, and cryptocurrencies to hide their activities and make anonymous payments, while law enforcement lacks forensic tools, skills, and

authority to access data; even when evidence is seized, poor handling candestroy it, and new threats like deepfakes make it harder to prove authenticity in court, according to digital forensics specialists cited by UNODC.

- **Capacity gaps, victim cooperation and legal fragmentation:** Many African countries lack trained investigators, digital forensic labs, and victim support systems, making survivors less likely to cooperate; according to INTERPOL's 2025 Africa Cyberthreat Assessment, **75%** of states admit weak legal frameworks, **95%** cite inadequate resources, only **30%** have reporting systems, and less than **20%** host cyber-threat databases, creating a wide gap between criminal sophistication and the ability to prosecute

Towards a survivor-centred cyber justice model

Africa's response to cyber-enabled child trafficking cannot rely only on punitive measures; instead, a survivor-centred cyber justice model should focus on prevention, early detection, victim support, and accountability by integrating technological capacity, harmonised laws, regional cooperation, and survivor-centred justice.

- **Building digital forensic capacity and specialised units:** Digital evidence underpins trafficking investigations, and according to INTERPOL, electronic evidence features in almost all crimes, making digital forensics, identifying, acquiring, analysing, and reporting on electronic data, essential; African states therefore need forensic labs that meet global standards, trained investigators, prosecutors and judges, and partnerships with universities and the private sector to strengthen capacity for decryption, crypto-tracing, and evidence authentication.

- **Harmonising laws and strengthening regional cooperation:** Effective cyber justice requires harmonised laws and data-sharing mechanisms; African states

should ratify and implement the AU's Malabo Convention on cybercrime and data protection and align laws accordingly, while regional bodies like ECOWAS, SADC, and the EAC should create digital-evidence frameworks and rapid response teams; internationally, engagement with the CLOUD Act and the Second Additional Protocol to the Budapest Convention is needed to ensure cross-border cooperation that reflects African realities.

- **Survivor-centred justice and reintegration:** Survivor-centred justice protects victims' rights, dignity, and recovery: according to the Disrupting Harm Project, only a tiny fraction of victims report abuse to police or helplines due to fear, shame, or

inaccessibility, so states should create child-friendly reporting channels (hotlines, apps, portals) and adapt trials with closed hearings, video testimony, and psychological support; General Comment No. 25 to the CRC further stresses safe, accessible reporting, while long-term reintegration must include counselling, education, livelihoods, and family support to prevent re-victimisation.

- **Engaging the private sector and raising public awareness:** Technology companies are vital partners: according to INTERPOL's Africa Cyberthreat Assessment, 89% of states identify poor private-sector cooperation as a major gap; platforms must therefore enforce age verification, deploy AI to detect

grooming and abusive content, remove illegal material quickly, and publish transparency reports; governments should regulate provider obligations, while public awareness campaigns must equip children, parents, and educators with online safety knowledge and challenge stigma, supported by multi-stakeholder bodies that coordinate evidence-based prevention

Recommendations

Child trafficking in Africa has been transformed by the digital era, where internet connectivity, social media, and mobile devices give groomers, networkers, travellers, and traffickers unprecedented reach, while socio-economic vulnerabilities make children easy targets; yet implementation of international and regional legal frameworks remains weak due to outdated laws, poor cooperation, anonymity tools, under-reporting, and limited forensic capacity.

- **Invest in digital forensics capacity and training:** Cyber-enabled trafficking cannot be prosecuted without strong evidence; governments should establish forensic laboratories, equip cybercrime units, and train investigators and judges, according to INTERPOL, which notes that electronic evidence features in almost all crimes, while universities and private partners can expand talent through scholarships and training.
- **Modernise and harmonise legal frameworks:** Some African countries don't have some form of data or privacy protection law, and most are outdated or fail to cover children's online environment; states must align with the Palermo Protocol, the Optional Protocol, and CRC General Comment No. 25, and regional bodies

like ECOWAS, SADC, and EAC should create model laws, mutual legal assistance frameworks, and specialised cyber courts.

- **Establish Africa-specific frameworks for cross-border cooperation:** The MLAT system is outdated, and African countries rarely use voluntary cooperation with service providers; the AU should negotiate with global technology companies to allow secure direct requests under safeguards, while regional bodies create portals for rapid evidence sharing, drawing on models like the U.S. CLOUD Act and the Budapest Convention's Second Protocol.

- **Create child-friendly reporting and survivor support systems:** Reporting remains minimal , according to the Disrupting Harm Project, only a tiny fraction of victims report online exploitation , so governments should provide hotlines, apps, and websites, ensure trials minimise trauma with video testimony and privacy protections, and deliver comprehensive services including shelter, counselling, education, and reintegration.

- **Hold technology companies accountable and raise public awareness:** Digital platforms must enforce age verification, automated detection, and fast removal of child abuse material; according to INTERPOL's Africa Cyberthreat Assessment, **89%** of states face barriers engaging the private sector, so governments should

regulate provider obligations, establish multi-stakeholder forums, and run public awareness campaigns, while the AU's Child Online Safety Policy (2024) emphasises corporate responsibility and digital literacy.

- **Enhance data collection, research, and evaluation:** Policy must be grounded in evidence: governments should integrate exploitation data into national surveys, improve reporting systems, and encourage partnerships between universities, NGOs, and tech firms; according to ACPF and ChildFund, cross-border data sharing and long-term studies are essential to reveal trends, survivor experiences, and programme impact.

Conclusion

The digital age has created new avenues for child trafficking in Africa, with traffickers exploiting social media, messaging apps, and cryptocurrencies, according to UNODC and the Disrupting Harm Project. Weak protections and under-reporting persist, as UNCTAD notes only **52%** of African states have data laws, and INTERPOL reports **75%** weak frameworks with **95%** lacking resources. A survivor-centred cyber justice model, building forensic labs, harmonising laws, improving cross-border cooperation, child-friendly reporting, and tech sector accountability, as urged in the AU's Child Online Safety Policy (2024), is essential to protect children and ensure digital innovation supports sustainable development.

Journal of Anti-Corruption Law

UNIVERSITY of the WESTERN CAPE

FACULTY of LAW

THANK YOU

BY: PAUL MUKIIBI