



The African Women's
Development and
Communication Network

Girls & Young Women-Led Assessment on Online Sexual Exploitation, Abuse & Technology-Facilitated Gender-Based Violence in Africa



ACKNOWLEDGMENT

This assessment on **Online Sexual Exploitation, Abuse (OSEA) and Technology-Facilitated Gender-Based Violence** is the result of the collective efforts, vision, and collaboration of many dedicated girls and young women across the continent.

We extend our deepest gratitude to all **She Leads Programme Girls and Young Women Advocates** from the seven program-implementing countries - **Ethiopia, Ghana, Kenya, Liberia, Mali, Sierra Leone, and Uganda**. Your advocacy and invaluable contributions were foundational in shaping this assessment. Special recognition goes to the She Leads Programme Pan-African Programme Advisory Board members from both the first and second cohorts for their exceptional leadership throughout the assessment process. We extend heartfelt appreciation to **Felicity Feleke**, a She Leads Young Woman Advocate of Ethiopia, for spearheading the idea, conceptualizing this assessment and for her commitment throughout the process.

Additionally, we would like to recognize the invaluable contributions of girls and young women advocates from the Southern regions of Africa and across the continent who participated in the data collection, consultations, interviews, data analysis, and validation. Your voices, advocacy, and lived experiences have been essential in shaping this assessment and ensuring that it reflects the diverse perspectives of girls and young women across the continent.

We acknowledge the exceptional contributions of the She Leads consortium partners: **ECPAT International, Plan International African Union Liaison Office, African Women's Development and Communication Network (FEMNET), Terre des Hommes Netherlands, and Defence for Children**, as well as the two implementing partners, **GIMAC Young Women Network and Horn of Africa Youth Network**. Special thanks go to **Bilisuma** from Plan International AU Liaison Office, **Willy, Sendrine, and Daniel** from ECPAT International, and **Nene** from FEMNET for your expertise, support, and collaboration throughout this process, which have been instrumental in enhancing the depth and quality of this assessment.

We also acknowledge the timely support of non-She Leads project-implementing organizations, whose contributions during various consultations and validation workshops have been invaluable, including **UYDEL** (Uganda), **EDA** (Ethiopia), **ACESEM** (Mali), **DCI** (Liberia, Ghana, and Sierra Leone), and **KAACR** (Kenya).

Finally, we would like to acknowledge **Raphaella** - the consultant, for her dedicated support in assisting the girls and young women throughout the data analysis process and in compiling this report.



FOREWORD

We, the She Leads Pan-African Programme Girls and Young Women Advisory, are proud to present this assessment on Online Sexual Exploitation and Abuse (OSEA) and Technology-Facilitated Gender-Based Violence (GBV). Authored by resilient African girls and young women, this report marks a pivotal step in tackling the urgent issue of technology-facilitated GBV and OSEA, which profoundly affect girls and young women across the continent. The report you are about to read is not just a collection of data, but a powerful call to action driven by the voices, lived experiences, and advocacy of the very individuals it seeks to protect— African women and girls.

The purpose of this assessment is to bridge the critical gap in understanding the extent and impact of technology-facilitated GBV and OSEA on girls and young women across the continent. Through this report, we aim to highlight the severity of this issue and advocate for urgent change at all levels— governments, civil society organizations, tech companies, and beyond. We believe this document is a powerful tool for evidence-based advocacy, enabling girls, young women, and organizations led by them to assert their rights and demand safer digital spaces.

At the heart of this work lies the understanding that we, the authors and participants, are not just researchers or advocates—we are girls and young women who have felt the effects of this violence firsthand. This report is born out of our shared experiences, our struggles, and our deep commitment to seeing a world where girls and young women can thrive online without the fear of exploitation or harm. We demand it because we know it is within reach.

As you read this report, we urge all stakeholders—governments, NGOs, tech companies, and the broader public—to recognize the urgency of addressing this issue. Let this report inspire meaningful action and policy reform that will lead to a safer, more inclusive digital world for the generations to come. This is not just our fight—it is the fight of every girl and young woman across the globe, who believes in her right to a life free from violence and exploitation. Together, we can make this vision a reality.

She Leads Pan-African Programme GYW Advisory Board Members (1st and 2nd cohorts)



TABLE OF CONTENTS

ACKNOWLEDGMENT.....	2
FOREWORD.....	3
LIST OF ACRONYMS.....	5
ABOUT THE SHE LEADS PROGRAMME.....	6
ABOUT THE ASSESSMENT.....	7
AT A GLANCE.....	8
OBJECTIVES, METHODOLOGY AND LIMITATIONS OF THE ASSESSMENT.....	9
KEY FINDINGS AND CHALLENGES.....	10
KEY RECOMMENDATIONS.....	15
BRIEF COUNTRY OVERVIEWS.....	18
DATA ON THE PREVALENCE, EXPERIENCES, AND IMPACTS OF ONLINE SEXUAL EXPLOITATION AND ABUSE, CYBERBULLYING, AND CYBERCRIME AFFECTING GIRLS AND YOUNG WOMEN IN SOUTHERN AFRICA.....	33
ANALYSIS OF THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION - MALABO CONVENTION.....	34



LIST OF ACRONYMS

- AHTCPU** Anti-Human Trafficking & Child Protection Unit
- APDP** Personal Data Protection Authority
- CSAM** Child Sexual Abuse Material
- GYW** Girls and Young Women
- ICT** Information and Communication Technologies
- OSEA** Online Sexual Exploitation and Abuse
- OCSEA** Online Child Sexual Exploitation and Abuse
- GBV** Gender Based Violence



ABOUT SHE LEADS PROGRAMME

She Leads is a joint programme from Plan International Netherlands, ECPAT International, Defence for Children – ECPAT the Netherlands (DCI-ECPAT), African Women’s Development and Communication Network (FEMNET), and Terre des Hommes the Netherlands (TdH-NL). The She Leads consortium, which runs from 2021-2025, aims to increase the sustained influence of girls and young women (GYW) on decision-making and the transformation of gender norms in formal and informal institutions. The consortium will achieve this goal by working through three interrelated domains:

- Civil society domain: the enhancement of collective action of girls and young women in a gender-responsive civil society;
- Socio-cultural domain: support by increased acceptance of positive social gender norms;
- Institutional domain: enabling meaningful participation of girls and young women in political and decision-making institutions.

The geographic focus of the programme is East Africa (Uganda, Ethiopia, Kenya), West Africa (Ghana, Mali, Sierra Leone, Liberia) and the Middle East (Lebanon, Jordan). In addition to programming in these countries, a considerable part of the programming is done at the regional level (beyond the programme countries), targeting regional institutions and other stakeholders operating at the regional level.

As part of the SHE LEADS Pan-African Regional Programme, ECPAT International, Plan International AU Liaison Office, FEMNET and other consortium partners aims to provide platforms for girls and young women to amplify their voices, participate in social change, and work actively and meaningfully to influence strategies for online child sexual exploitation and abuse and technology-facilitated gender-based violence at the regional and global levels.



ABOUT THE ASSESSMENT

The girls and young women-led assessment on Online Sexual Exploitation and Abuse, Cybercrime and Cyberbullying is an initiative that was spearheaded by the She Leads Project Girls and Young Women Advisory Board Members aiming to advocate for the reduction, if not eradication of the growing risks, vulnerabilities and harms the youth, particularly girls and young women, face online in the region. The assessment takes place in seven countries: Ethiopia, Ghana, Kenya, Liberia, Mali, Sierra Leone and Uganda.

The decision by the girls and young women involved in the She Leads GYW Advisory Board to focus on Online Sexual Exploitation and Abuse and Technology-facilitated Gender Based Violence was driven by their lived realities and a pressing need to address the unique challenges they face

in the digital space. As online sexual exploitation, become more prevalent, girls and young women saw an urgent need to address these issues at a systemic level, ensuring that solutions are locally relevant while aligned with global standards for digital safety. Despite increasing evidence of the disproportionate impact of online risks on this demographic, there remains a gap in gender-disaggregated data to fully understand and address these issues effectively. Girls and young women also recognised that the risks and impacts of online sexual exploitation and abuse are often shaped by societal gender norms, with girls and young women disproportionately targeted due to their gender. This includes receiving more frequent and severe harassment, online sexual exploitation and cyberattacks, which often go unnoticed or unaddressed in mainstream discussions.

Moreover, existing policies and OCSEA-related research often fail to consider the specific needs and experiences of girls and young women, leading to interventions that are either ineffective or exclude them altogether. By focusing on this issue, girls and young women aim to fill a critical gap in knowledge and advocacy. As active users of digital spaces for education, activism, and networking, girls and young women see the internet as a vital tool for empowerment. However, the lack of safety and accountability in these spaces undermines their ability to fully participate and thrive online. They want to highlight these issues and advocate for solutions that would ensure safer digital environments for themselves and future generations.



AT A GLANCE

The report highlights the significant challenges that girls and young women (GYW) face in the digital space regarding OCSEA and technology-facilitated gender-based violence across seven countries in Africa. Girls and young women experience significant online violence, including cyberbullying and the non-consensual sharing of intimate content, often exacerbated by entrenched gender norms that normalise violence and harassment against girls and women. Many girls and young women lack knowledge about digital literacy, online safety and reporting mechanisms, with this knowledge not being properly disseminated, especially in rural areas, making them more vulnerable to exploitation. Cultural barriers also contribute to the issue, with societal stigmas and victim-blaming preventing many victims from reporting incidents of online violence. The study highlights major shortcomings, including ineffective reporting mechanisms and inadequate legal protection. Legal frameworks in place often fail to adequately criminalise all forms of OCSEA-related offences, and enforcement mechanisms are hampered by a lack of technical expertise and resources. This legal insufficiency is aggravated by underreporting, as there is a lack of effective, widely accessible reporting mechanisms, and victims face a lack of trust in the legal system, fearing that justice will not be served, leading to impunity for offenders.

The assessment offers a comprehensive set of key recommendations to tackle these challenges. Schools, families, and community organisations play a crucial role in combating OCSEA and technology-facilitated gender-based violence. Schools should work in collaboration with girls and young women to incorporate educational modules on OCSEA and technology-facilitated gender-based violence into curricula, promote initiatives led by GYW, and train staff to detect and respond to signs of abuse. Families are encouraged to foster open communication, support their children and educate themselves about digital literacy, digital rights and online safety. Civil society organisations should engage youth organisations to raise awareness, promote cultural change, and develop nationwide digital safety campaigns targeting girls and young women. Efforts should focus on equipping parents with the skills to protect their children online, train local leaders, and enhance the role of community organisations in providing support, particularly in rural areas.

Dedicated local reporting and support centers should be established, along with raising awareness about existing resources such as national helplines. Collaboration between civil society, communities, and law enforcement is crucial for effective prevention and response. Governments are urged to adopt and implement legislation that fully criminalises all forms of OCSEA and technology-facilitated gender-based violence, with provisions recognising the specific needs of girls and young women. This legislation must be accessible and widely disseminated in local languages throughout the country, with the involvement of youth organisations. Additionally, governments should engage girls and young women in the development and review of digital policies, legislation and educational programmes. It is also strongly recommended that governments establish an effective and accessible national helpline equipped to deal with OCSEA and technology-facilitated gender-based violence. Other relevant stakeholders in the digital space should collaborate with girls and young women, civil society organisations, and governments to enhance digital safety. This involves developing educational programmes and media campaigns to promote safe online behaviours, implementing stricter cybersecurity policies, and establishing regulations for digital platforms to filter harmful content and hold perpetrators accountable. Stakeholders are encouraged to create safer digital platforms and improve support services and reporting mechanisms.



OBJECTIVES, METHODOLOGY AND LIMITATIONS OF THE ASSESSMENT

The objectives of the assessment include:

1. **Addressing the research gap:** The existing research landscape on online child sexual exploitation and abuse, and online violence often lacks sufficient disaggregation by gender to assess the specific experiences of girls and young women. The primary objective of this assessment is to fill this gap and shed light on the experiences of girls and young women in relation to OSEA and Technology-facilitated Gender Based Violence in Africa.
2. **Understanding the impact of online sexual exploitation and abuse on girls and young women:** The hindrance faced by girls and young women in participating in virtual platforms due to multiple online risks underscores the urgency and importance of this assessment. The assessment aims to gain a comprehensive understanding of the impact of these online risks on girls and young women in Africa.
3. **Generating evidence-based advocacy:** The collaborative effort of girls and young women across the seven countries where the She Leads program operates holds promise in generating comprehensive data. The assessment strives to inform policies and interventions that promote their safety, well-being, and empowerment in the digital space.

A data collection strategy has been developed by the girls and young women that incorporates various methods for gathering insights and information on online child sexual exploitation, cyberbullying, and cybercrime in the seven countries.

- **Online Surveys:** Gathering anonymous responses from 109 girls and young women aged 15 to 24, to identify problems and countermeasures in schools and universities.
- **Literature Review:** Examine existing policies, laws, cybersecurity acts, research, and legal frameworks on online child sexual exploitation and abuse.
- **Key Informant Interviews:** Conducting key informant interviews with 100 stakeholders from government agencies and civil society organisations working in the field of OCSEA, cyberbullying and cybercrime.

The assessment was entirely led and implemented by girls and young women, reflecting their direct experiences and perspectives. It is important to note that the assessment has limitations in terms of data collection, scope, and analysis. The findings do not aim to be comprehensive academic research, but rather an assessment offering valuable insights based on the lived experiences of girls and young women across seven countries in Africa. The purpose of this work is to provide a starting point for engaging policymakers and raising awareness on online sexual exploitation and technology-facilitated gender-based violence emphasising the urgent need for action in these areas.



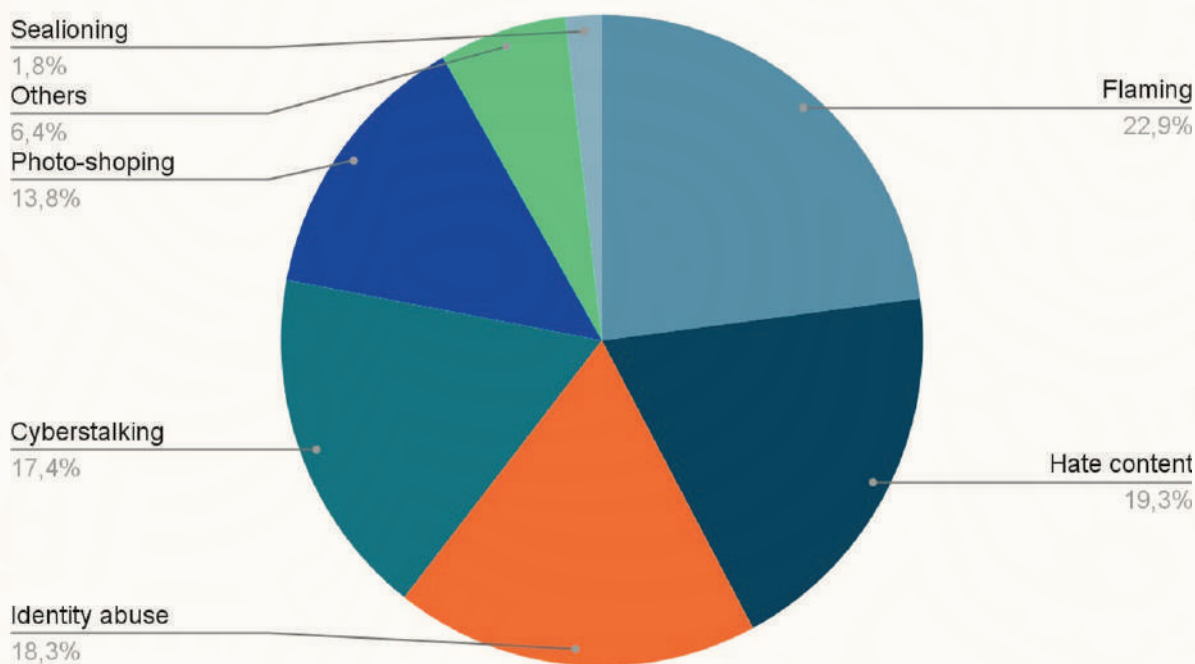
KEY FINDINGS AND CHALLENGES

1. Normalisation of Technology-Facilitated Gender-Based Violence in the Region

Across Africa, girls and young women face unique challenges related to technology-facilitated gender-based violence. Instances of non-consensual sharing of intimate content, cyberbullying, and online harassment disproportionately impact them and have serious emotional, psychological, and social consequences. Girls and young women who took part in the online survey reported that Facebook, TikTok and Instagram are the main online platforms used, closely followed by Twitter (X) and Snapchat. They also noted that abuse is increasingly prevalent on Telegram and WhatsApp. 63% of the girls and young women surveyed have experienced online harassment on these platforms.

Flaming¹ (22,9%) is the most common type of online harassment reported by girls and young women who took part in the online survey, accounting for almost a quarter of responses. Hate content² (19,3%), identity abuse³ (18,3%) and cyberstalking (17,4%),⁴ are equally significant issues. This indicates a high prevalence of repetitive and malicious online behaviour aimed at intimidation and damage to reputation. Photo-shopping,⁵ though less common, still affects a significant portion of girls and young women respondents (13,8%) and is becoming the norm of the day. Finally, sealioning⁶ is relatively rare (1,8%) compared to other forms of harassment, but its presence in the data suggests it is still a relevant issue.

What type of online harassment is more common?



The constant exposure to hateful comments, threats, and insults, often related to their appearance, lifestyle, economic status, or ethnicity, impact their self-esteem, cause body image issues, and lead to feelings of inferiority and insecurity. In extreme cases, the mental toll of constant online harassment can lead to depression, loss of motivation and suicidal thoughts. Overall, the impact of online abuse is

¹ **Flaming** - When a person sends angry, rude, or obscene messages directed at a person or persons privately or an online group.

² **Hate content** - When a person makes hateful posts and messages about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender, with the intention to damage someone's reputation.

³ **Identity abuse** - when someone steals and uses your personally identifiable information to defraud or harm you

⁴ **Cyberstalking** - When a person keeps constant track of someone online in a way that makes them feel uncomfortable, worried or threatened.

⁵ **Photo-shopping** - When a person alters a digital image so that the main subject is placed in compromising or embarrassing situations.

⁶ **Sealioning** - When a person insistently seeks information in order to provoke an irate reaction.



profound, affecting their mental health, sense of safety, and ability to pursue their dreams, passions and ambitions. Early pregnancies and school dropouts are common, as girls and young women face social isolation and lose educational opportunities. Many young girls feel unsupported by families, community structures and religious institutions.

Poverty has been highlighted as a major factor fuelling online abuse. Many girls and young women remain vulnerable because they believe that online strangers can improve their economic situation. Participants expressed concern about platforms such as Strip Chat and OnlyFans, where adults exploit young people for profit by using them to attract more viewers and earn more money.

Two-thirds of the girls and young women reported being exposed to instances of OCSEA and technology-facilitated gender-based violence such as being frequently exposed to inappropriate content on online platforms or receiving photos of a sexual nature without their consent, with the sender often requesting nude photos in exchange. Many girls and young women have reported being victims of non-consensual sharing of intimate content, finding themselves in

situations where, after sharing personal photos or videos with people they trusted, these same people either shared the photos to get back at them or blackmailed them into doing something or sharing certain information under the threat of sharing online these personal photos and videos. Blackmail and manipulation to share explicit content under false pretences such as a promise of a job or a romantic relationship are widespread. Reputational damage is common, particularly when intimate content is shared widely, leading to severe emotional distress, social stigma and exclusion from communities and/or schools. Online hate comments are also a common form of cybercrime and many victims end up closing their accounts and feeling insecure offline and online. Finally, hacking and identity abuse, to extort money from family members and relatives, were also reported by many girls and young women. The intersectionality of gender and technology often results in the perpetuation of harmful stereotypes and unequal power dynamics, hindering the empowerment of girls and young women in the digital space.

2. Social Stigmas Blaming the Victims

A recurring theme is the difficulty in overcoming cultural and social stigmas that discourage victims from speaking out. Social stigmas often lead to harassment being rationalised as a consequence of a girl or young woman's behaviour, discouraging them from reporting. When girls and young women seek help, they frequently encounter a lack of understanding of the severity of the abuse from law enforcement and support services. Frontline workers may not fully grasp the impact of the abuse when it occurs online or through technology. There is also a lack of belief from their friends and family, with some people dismissing their experiences or telling them they "like what's going on". Parents often lack the skills to understand and support their children, preferring to settle the matter privately with the offender. OCSEA and technology-facilitated gender-based violence are often disregarded as not as serious as other forms of violence such as contact abuse, and do not receive the same level of attention by professionals who are also not fully aware of the linkages with contact offending or the impacts on the victims. They are poorly equipped to support victims or to lead investigations on these issues, which leads to a lack of accountability on the part of the perpetrator and a feeling of impunity and tolerance for these crimes.

Girls and young women fear backlash and shame, particularly from members of their family and community, especially if they have done something like sharing a sexualised image. Because of cultural and social stigmas, people tend to see them as responsible for the violence they suffer, rather than recognising the offender who took advantage of a situation and manipulated the victim into the abuse. These public perceptions and attitudes contribute to a culture of blaming and shaming victims, and maintaining them into silence. It contributes to social acceptance of the phenomenon which perpetuates technology-facilitated gender-based violence in the region.



3. Relations to the Offenders

As the findings of the *Disrupting Harm* research highlighted, children who have experienced online child sexual exploitation and abuse are likely to have already known the perpetrator – a friend, acquaintance, family member or romantic partner. While a common stereotype is that strangers are the main perpetrators of online child sexual exploitation and abuse, children’s responses reveal that these acts are more often committed by people they know.⁷ In these contexts, fear of retaliation is a significant issue, particularly if the offender is a prominent figure in the community or close to the victim, which makes reporting even more difficult.

Girls and young women who took part in the online survey shared that many victims know their abusers personally, as in the cases of cyberstalking by classmates or harassment by authority figures such as teachers. However, girls and young women also stressed that while it is common for victims to know their abusers, it is also important to bear in mind that the Internet multiplies the opportunities for strangers to sexually exploit and abuse girls and young women.

4. Education and Awareness of OSEA and Technology-Facilitated Gender-Based Violence

Lack of education on digital literacy and online safety targeting girls and young women

Girls and young women who took part in the online survey provided diverse yet insightful definitions of cybercrime and online child sexual exploitation, highlighting the complexity of these issues. Participants seemed aware of some of the risks associated with online activities. Yet, most girls and young women do not seem to be aware of all forms of cybercrimes and online abuses. Only half of the girls and young women surveyed reported having received any formal, or informal education or training on digital literacy, cybersecurity, or online safety.

According to respondents to the assessment working in civil society organisations, girls and young women have limited knowledge of laws, policies, and mechanisms related to cybercrime and online child sexual exploitation and abuse. While some girls and young women are informed— particularly those involved in mentorship programs, advocacy, or specific community initiatives— many others, especially in rural areas and marginalised communities, lack knowledge of OCSEA and technology-facilitated gender-based violence.

Girls and young women lack knowledge of digital literacy and online safety, which prevents many victims from making effective use of reporting mechanisms, particularly in rural and marginalised communities. Due to low levels of digital literacy, girls and young women are more exposed to online sexual exploitation and abuse, and technology-facilitated gender-based violence, being unable, for example, to properly adjust their phone’s privacy settings.

Cultural and family barriers, such as the inability to discuss online sexual exploitation and abuse, and technology-facilitated gender-based violence openly, make it harder for many girls and young women to seek help, leaving them vulnerable to further sexual exploitation and violence. Often, families of victims and survivors have limited understanding of OCSEA and technology-facilitated gender-based violence. Parents and guardians suffer from a lack of knowledge about digital literacy, digital rights and online safety. Parental involvement and control is often absent and inadequate to support and protect children.

Lack of awareness-raising and education campaigns reaching girls and young women

The majority of the respondents involved in civil society organisations who participated in the assessment reported that their organisation runs some awareness campaigns on cybercrimes and online child sexual exploitation targeting GYW. These initiatives include radio advocacy, posters, awareness campaigns,

⁷ UNICEF Innocenti – Global Office of Research and Foresight (2023). [Who perpetrates online child sexual exploitation and abuse?](#) Disrupting Harm Data Insight 8, Safe Online. End Violence Partnership, UNICEF, 2023



community outreach, online webinars, digital and social media campaigns, as well as in-person educational sessions aimed at girls and young women, their families and communities.

However, they also highlighted the inadequate dissemination of knowledge, relevant legislation, and protective rights related to OCSEA and technology-facilitated gender-based violence across the country. The issue extends to reporting mechanisms as well, with a lack of information about reporting centres and the procedures for reporting abuses, which remains one of the primary barriers to reporting. Information is typically shared through schools, community forums, workshops, social media, and training. However, many girls, especially those in remote areas and/or with special needs, are not exposed to this vital information. It was pointed out that school staff lack knowledge about digital literacy and online safety, and school curricula often do not include a programme on online safety nor OCSEA. Additionally, the materials that are available are often not translated into local languages or tailored to girls and young women's literacy levels. Efforts are often inconsistent and limited by barriers such as poor access to technology and organisations' lack of technical and financial resources to implement such initiatives.

5. Safe Online Practices Used by Girls and Young Women

Faced with these risks, girls and young women have adopted practices to protect themselves from exposure to unwanted and harmful experiences online. Girls and young women who took part in the online survey shared a range of precautions they take to safeguard their well-being while using the internet, including blocking or restricting unwanted contacts and content, avoiding sharing personal information, such as location or phone numbers, and reporting inappropriate content or users. Participants said they were careful about limiting their time on the internet, ensuring their social media accounts are set to private, avoiding talking to strangers online and prioritising the use of strong passwords. Some participants also mentioned taking extra steps such as verifying friend requests, being mindful of what content they share online and avoiding unverified content. Only a few participants mentioned using antivirus software, regularly updating applications, and being cautious about clicking on links or downloading files. Finally, participants indicated that peer support was very important when faced with any form of online violence.



6. Perceived Impunity of Offenders and System Failure Discourage in Reporting and Access to Justice

In general, there is a lack of effective, well-known, trusted and widely accessible reporting mechanisms accessible for victims of OCSEA and technology-facilitated gender-based violence. The issues of OCSEA and technology-facilitated gender-based violence remain largely underreported. The complexity of reporting processes across different platforms, the absence of clear guidance and support from authorities, corruption within the police force, and the lack of specific laws criminalising online violence all contribute to a discouraging environment for victims. These challenges are further compounded by the stigma and shame associated with reporting. Additionally, there is a lack of technological capacity and limited awareness among law enforcement and criminal justice professionals, further hindering effective responses. Finally, the complexities of addressing online violence due to the difficulty in tracing and identifying perpetrators, absence of coordination and clear policies between countries, weak law enforcement, and delays in justice contribute to a slow and inadequate response.

Respondents working in organisations also highlighted the lack of coordination, awareness as well as technical and financial resources within organisations, which prevents their ability to respond effectively. Marginalised communities, especially rural areas, face limited access to technology and digital tools, further hindering their ability to protect themselves or report incidents effectively.

Many girls and young women surveyed expressed their frustration with the lack of accountability and follow-through, noting that even when they report abuse, they rarely receive responses or see any legal action taken against the perpetrator. There is a lack of trust in the available services and concerns about security and privacy when reporting. The anonymity of online abusers, who often hide behind fake profiles, makes it difficult to identify the person responsible. As a result people often tend to ignore the abuse and not seek help. Only half of them have ever reported an online incident that threatened their well-being. In addition, participants pointed out that the financial costs and distance of the services available, which tend to be centralised in urban areas, prevent girls and young women living in rural areas and marginalised communities from reporting.



KEY RECOMMENDATIONS

The role of schools, families and community organisations in the fight against OCSEA and technology-facilitated gender-based violence:

Schools: Educate, Raise Awareness and Protect

- Develop, with the participation of girls and young women, modules on OCSEA and technology-facilitated gender-based violence, and include them in school and university curricula.
- Promote, facilitate and support girl- and young woman-led initiatives (workshops, debates, etc.) in schools and universities to teach students about digital literacy, digital rights and online safety.
- Train teachers and school staff to detect signs of OCSEA and technology-facilitated gender-based violence and to respond effectively.
- Establish contact points and youth-led safe spaces in schools and universities to ensure that victims have access to support and to facilitate reporting.
- Guarantee safe access to technology by installing filters on school networks to limit students' exposure to inappropriate content.
- Support and encourage children and youths to contribute to the design, implementation and monitoring of protection and response systems adapted to their needs, practices and contexts.
- Link the schools' and universities' reporting and response system to the public response system to ensure an immediate and appropriate response to victims of OCSEA and technology-facilitated gender-based violence.

Families: Prevent and Support

- Learn more about digital literacy, digital rights and online safety.
- Supervise the use of digital devices, implementing safety measures, and teach children about online risks and safety.
- Foster an open and positive relationship with their children to facilitate honest communication and encourage discussions at home about online safety.
- Learn to identify signs of trauma and abuse, and seek professional help if necessary.
- Support children in their efforts to report any incident, without judgement or guilt.

Civil Society Organisations and Communities: Mobilise, Raise Awareness and Protect

- Engage youth organisations to raise community awareness of OCSEA and technology-facilitated gender-based violence, and to promote cultural and societal change to challenge harmful gender and sexual norms and attitudes.
- Collaborate with girls and young women to create, implement and monitor nationwide digital safety awareness campaigns, including through social media outreach and community dialogues.
- Equip parents with skills to educate their children about digital rights and online safety, as well as how to protect and support them.
- Train local leaders and people working in civil society organisations on OCSEA and technology-facilitated gender-based violence, and how to respond effectively.
- Strengthen the role of community organisations in raising awareness on OCSEA and technology-facilitated gender-based violence, and providing local support services for girls and young women, particularly in rural areas.
- Establish dedicated local reporting and support centres for girls and young women facing OCSEA and technology-facilitated gender-based violence, and disseminate their existence.



- Raise awareness about the national helpline and other reporting systems as a source of information and support for girls and young women subjected to OCSEA and technology- facilitated gender-based violence.
- Provide youth-led safe spaces in the community where young people can talk about their experiences and learn how to protect themselves.
- Strengthen the collaboration on prevention and case reporting between girls and young women, civil society organisations, communities and law enforcement agencies to address OCSEA and technology-facilitated gender-based violence.

The role of governments in strengthening the legal framework, implementing new programmes and enhancing support systems:

Policy and Legal Frameworks: Strengthening and Implementing

- Adopt and implement relevant legislation that explicitly and fully criminalises all forms of OCSEA and technology-facilitated gender-based violence related offences, with rightful penalties and including provisions that explicitly recognise the specific rights and needs of girls and young women.
- Ensure that the relevant legislation is made available in a format that is accessible and understandable to girls and young women, translated into local languages and widely disseminated throughout the country with the involvement of youth organisations.
- Actively involve girls and young women in the development and review of digital policies and legislation to ensure that their perspectives and needs are taken into account.
- Establish strong international collaboration and cooperation to combat cross-border online threats.
- Ratify and domesticate the African Union Malabo Convention on Cybersecurity and Personal Data Protection to establish a unified legal framework addressing cybersecurity and online abuse.

New Programmes: Developing and Training

- Engage girls and young women in the drafting of a comprehensive national education programme to raise awareness on OSEA and technology-facilitated gender-based violence.
- Launch a government-supported program to designate girls and young women as Digital Safety Ambassadors, enabling them to raise awareness, advocate for online safety, and influence policy-making.
- Train law enforcement officers, criminal justice professionals and the frontline social service workforce on OSEA and technology-facilitated gender-based violence, and how to respond to it effectively and sensitively, integrating gender perspectives.
- Implement guidelines on interviewing children and women during the criminal justice process.
- Provide funding to public and private institutions that offer support services to victims of OSEA and technology-facilitated gender-based violence.

Reporting Systems: Accessibility and Sustainability

- Ensure an effective accessible free 24/7 national helpline equipped to deal with OSEA and technology-facilitated gender-based violence, and disseminate its existence.
- Ensure accessible psychological support and legal recourse throughout the country for victims of OSEA and technology-facilitated gender-based violence.
- Collect data and monitor OSEA and technology-facilitated gender-based violence cases, including the collection of gender-disaggregated data, on the national and local levels.



The role of other relevant stakeholders in the digital space in the fight against OSEA and technology-facilitated gender-based violence:

Digital education: Educate and Raise Awareness

- In collaboration with girls and young-women, develop and disseminate educational programmes to teach young people how to use digital tools and be safe online.
- In collaboration with girls and young-women, launch media campaigns to portray positive images of young girls and women and raise awareness about OSEA and technology- facilitated gender-based violence.
- Engage in partnerships and work with civil society organisations and communities to organise activities in schools, universities, workplaces and communities OSEA and technology-facilitated gender-based violence.

Digital regulation: Online Protection and Security

- Collaborate with girls and young women, civil society organisations, communities and governments to the development and implementation of stricter cybersecurity policies.
- Establish and implement a framework against OSEA and technology-facilitated gender- based violence within their scope of operations.
- Establish strict regulations of digital platforms and applications to strengthen authentication methods to platforms, develop content filtering tools to limit children's exposure to harmful content, monitor such content and hold perpetrators accountable.
- Impose real restrictions on access to certain platforms based on age, to protect young users from potential risks.
- Systematically suggest installing parental controls to limit children's access to harmful content.

Digital support: Tailored Online Tools and Services

- In collaboration with girls and young women, develop safer digital platforms and applications.
- In collaboration with girls and young women, develop and improve support services and reporting mechanisms.
- Provide feedback on reports of online abuse, to foster trust and encourage reporting by users.
- Provide simpler and more child-friendly terms and conditions on digital platforms and applications.
- Offer online psychological support services for young people affected by OSEA and technology-facilitated gender-based violence.
- Fund digital initiatives and projects developed by girls and young women on OSEA and technology-facilitated gender-based violence



BRIEF COUNTRY OVERVIEWS

ETHIOPIA



CONTEXT

In 2021, 10% of internet-users aged 12–17 in Ethiopia were victims of serious cases of online child sexual exploitation and abuse, this represents an estimated 300,000 children. According to the Disrupting Harm research: ‘This includes blackmailing children to engage in sexual activities, sharing their sexual images without permission, or coercing them to engage in sexual activities through promises of money or gifts’.⁸ Incidents of gender-based violence against women and girls are occurring in Ethiopia, as the vast majority (89%) of victims of child sexual exploitation recorded by the Ethiopian national authorities in recent years have been girls.⁹ As another example, in 2017, the ECFA Ethiopia helpline reported receiving 70 contacts relating to OCSEA, all of which concerned girls and related to the online distribution of child sexual abuse material (CSAM) and grooming.¹⁰ Although qualitative studies suggest that cyberbullying is an emerging issue and awareness of cybercrime is growing, specific data on incidence rates among girls and young women is scarce.

Awareness and understanding of OCSEA by children and the general public are low as well as among Ethiopian policymakers and frontline workers.¹¹ According to the Disrupting Harm research, only 37% of children reported that they had ever received information on online safety, including how to handle online harassment, what content to avoid sharing, and how to adjust their privacy settings.¹² In addition, according to a representative from the Directorate of Women, Children, and Youth in the Ministry of Innovation and Technology in Ethiopia, there is a lack of understanding and awareness about OCSEA in the country.¹³ Some initiatives exist such as the Yellow Movement who recently launched a project aimed at raising awareness about cybercrime and promoting digital literacy.

Most incidents of attempted or actual OSEA and technology-facilitated gender-based violence are not officially reported in Ethiopia. There are several reasons for this: the lack of awareness about where or how or whom to tell, fear of shame, stigma or victim blaming, lack of knowledge of OSEA as a rights violation, and lack of confidence in the police and other support services.¹⁴

LEGAL FRAMEWORK AND LAW ENFORCEMENT RESPONSE

The existing national laws relevant to OSEA-related crimes in Ethiopia are the Computer Crime Proclamation (2016) and The Criminal Code (2005). However, these laws only partially criminalise grooming and do not specifically criminalise online sexual extortion, online sexual harassment, or the live-streaming of child sexual abuse. Laws also didn’t incorporate gender perspectives in provisions that explicitly recognise the rights and specific needs of girls and young women.

Regarding law enforcement response, there is no specific agency or plan to specifically address OCSEA cases in Ethiopia nor technology-facilitated gender-based violence. Although there is a dedicated online crime unit, to date (2021), no OSEA-related cases have been referred to them, except cases of sexual extortion of women that sometimes involve children.¹⁵ Law enforcement officials reported zero OSEA-

8 ECPAT, INTERPOL, and UNICEF. (2022). [Disrupting Harm in Ethiopia: Evidence on online child sexual exploitation and abuse](#). Global Partnership to End Violence against Children. 7.

9 Ibid, 58.

10 Ibid, 61.

11 ECPAT, INTERPOL, and UNICEF. (2022). [Disrupting Harm in Ethiopia: Evidence on online child sexual exploitation and abuse](#). Global Partnership to End Violence against Children. 21.

12 Ibid, 21.

13 Ibid, 21.

14 Ibid, 62.

15 ECPAT, INTERPOL, and UNICEF. (2022). [Disrupting Harm in Ethiopia: Evidence on online child sexual exploitation and abuse](#). Global



related cases.¹⁶

In addition, according to a representative from the Ministry of Women and Social Affairs, criminal justice professionals in Ethiopia have limited technical knowledge and awareness when it comes to investigating, prosecuting, and adjudicating OSEA cases. There is a cyber forensics unit that deals with all cases of cybercrime, but there are no law enforcement officers dedicated to investigating OSEA. In terms of adopting a victim-centred approach, some courts have child-friendly benches.¹⁷

At all levels, there is a lack of trained professionals, capacity, equipment, and technical expertise on OSEA and technology-facilitated gender-based violence.¹⁸

No information is to be found on cases of girls or young women victims of OSEA and/or technology-facilitated gender-based violence successfully securing compensation.



Partnership to End Violence against Children. 64.

16 Ibid, 64.

17 Interview conducted by the SheLeads Team to a key informant from the Ministry of Women and Social Affairs in Ethiopia.

18 Ibid, 65.



GHANA

CONTEXT



Cases of OCSEA and technology-facilitated gender-based violence, especially targeting girls and young women, are occurring in Ghana. In 2024, the African Child Policy Forum and ChildFund International indicated that up to 65% of the victims of OCSEA in Africa are girls, with the sexual exploitation affecting them at very young ages.¹⁹ A 2023 UNICEF study also focused on adolescent girls in Ghana that revealed that the COVID-19 pandemic exacerbated these challenges by pushing more activities online. As a result, vulnerable adolescent girls faced heightened risks, including sexual and gender-based violence, and online harassment, which impacted their mental health and well-being.²⁰

Cyberbullying is recognised as a significant issue in Ghana, impacting young people through various forms of digital abuse. For instance, a publication, by the International Journal of Computer Applications, in 2022, underscore the harmful effects of cyberbullying on youth and highlight the growing challenges schools and communities face in addressing it.²¹

Furthermore, in 2022, the Cyber Security Authority conducted a survey in schools revealing that out of 3600 children interviewed, 2331 had received sexual content online with the same number of them having met physically a stranger they had first met online, 1418 had experienced romance scam, and 862 had been scammed and required to provide sex.²²

Ghana has taken the fight against OCSEA very seriously, being one of the first country to launch a Child Online Protection Reporting Portal in 2020, through the National Cyber Security Centre, providing a safe platform for people to report suspected child sexual abuse materials.²³

In addition, emergency hotlines exist such as those provided by the Domestic Violence and Victim Support Unit for victims to call and report incidents. In some communities, there are also initiatives like “See Something, Say Something,” which encourages individuals to report online abuses.

Campaigns aiming to raise awareness about the growing issue of online child sexual exploitation and abuse have been undertaken.²⁴ In Ghana, organisations actively involved focus on promoting female leadership and digital literacy, helping young women to learn how to safely navigate social media and use it to their advantage. Other organisations run online and physical campaigns against cyberbullying, raising awareness through radio advocacy, community engagement, and programs that educate about the dangers of cybercrimes. For example, an organisation has conducted educational campaigns reaching over 100 women and girls in both rural and urban areas, focusing on online safety and how to report cyberbullying. Another one hosted youth symposiums and mentorship programs, reaching 300 girls and young women. Finally, a few organisations offer referral services, directing victims of online abuse to the appropriate departments for further support.

However, the limited awareness of OCSEA and technology-facilitated gender-based violence among the public, law enforcement, government officials, the families of victims and survivors continues to be a major barrier to reporting.²⁵

19 ChildFund International and African Child Policy Forum. (2024, May 30). [Online exploitation and abuse of children in Africa on the rise](#). ChildFund Alliance.

20 Owusu-Addo E and Owusu-Addo SB (2022). [The Impact of COVID-19 on Adolescent Girls' Sexual and Reproductive Health and Rights: A Mixed-Method Study](#). UNICEF Ghana, Accra.

21 International Journal of Computer Applications (0975 – 8887) Volume 183 – No. 48, January 2022.

22 Times Ghanaian. (2019, June 19). [CHRAJ advocates implementation of laws to make internet safer for Ghanaian children](#). Times Ghanaian.

23 Zadok Kwame Gyasi. (2020, October 01). [Ghana launches Child Online Protection Reporting Portal](#). Graphic Online.

24 UNODC. (2023). [UNODC launches the 'Safer Children Online' campaign to combat online child sexual exploitation and abuse in Ghana and Senegal](#).

25 ECOWAS Commission. (2023, Augst). [Online child sexual exploitation and abuse in West Africa](#). 4.



LEGAL FRAMEWORK AND LAW ENFORCEMENT RESPONSE

The existing national laws relevant to child rights in Ghana include: Criminal Code, 1960 (ACT 29), Children's Act, 1998 (Act 560), Juvenile Justice Act, 2003 (ACT 653), Electronic Transaction Act, 2008 (Act 772), Data Protection Act, 2012, Criminal Offences (Amendment) Act, 2012 and Cybersecurity Act (2020). However, those laws don't explicitly and fully criminalise all forms of OCSEA-related offences nor include provisions that explicitly recognise the rights and specific needs of girls and young women.²⁶

In October 2024, the Cyber Security Authority launched the National Child Online Protection Framework.²⁷ The framework seeks to provide a safe and empowering online experience for children in Ghana as well as guiding the Government, Industry, Civil Society Organisations, Educators, Parents and other relevant stakeholders to efficiently protect children from all forms of online abuse.

However, at present, there is still a clear lack of awareness on OCSEA and technology-facilitated gender-based violence, inadequate resources, poor coordination between agencies and organisations and insufficient training.²⁸ No specific agency or unit to specifically address OSEA cases in Ethiopia nor technology-facilitated gender-based violence.

No information is to be found on cases of girls or young women victims of OSEA and/or technology-facilitated gender-based violence successfully securing compensation.



26 Ministry of Gender Children and Social Protection. (2018, July). [Position paper on children's online safety concerns in Ghana](#). 14.

27 Edward Dankwah. (2024, October 22). [Child Online Protection Framework launched in Accra](#). GNA Ghana News Agency.

28 ECOWAS Commission. (2023, Augst). [Online child sexual exploitation and abuse in West Africa](#). 4.

KENYA

CONTEXT



In 2024, the African Child Policy Forum and ChildFund International indicated that up to 13% of 12–17-year-olds in Kenya and Mozambique were threatened or blackmailed to engage in sexual activities online.²⁹

In 2019, the Anti Human Trafficking and Child Protection Unit (AHT CPU) of the Kenyan National Police Service reported 4,133 cases of OCSEA. Unfortunately, OCSEA cases are not always broken down by gender.³⁰ According to the Kenyan section of the International Commission of Jurists, research indicates that more than one in five women in Kenya reported having experienced online harassment.³¹ Furthermore, a survey conducted by the Collaborative Centre for Gender and Development in partnership with the University of Nairobi Women’s Economic Empowerment Hub and with UNFPA, showed that the platforms where technology-facilitated gender-based violence mainly occur are X (formerly Twitter), WhatsApp, Facebook and Telegram. In addition, the study found that female students were more affected, with 64.4% of female students experiencing at least one type of online violence.³²

In Kenya, several reporting mechanisms are available for victims of online abuse, including the Safe City app, the Internet Watch Foundation Kenya portal, toll-free helplines, the National KE- CIRT, and police stations. However, they lack financial and human resources to adequately respond to OCSEA and technology-facilitated gender-based violence.³³ Most cases of OCSEA are not officially reported in Kenya, this is due to a fear of potential negative consequences, a fear of not being treated properly by the authorities, a lack of trust in the services and a belief that reporting would have no effect.³⁴ In 2019, the hotline Childline Kenya 116 reported that OCSEA cases made up only 2% of total contacts received.³⁵

Awareness and understanding of OCSEA and technology-facilitated gender-based violence by the general public in Kenya are low.³⁶ However some organisations are actively involved in the fight against cybercrimes, and OCSEA targeting girls and young women. Some focus on creating safe spaces for GYW to discuss their issues, while others provide capacity-building workshops, teaching GYW how to identify and respond to cyberbullying and online sexual exploitation. Organisations like Polycom Development Project and Women Aspire Network use social media (e.g., Twitter) and online platforms to spread awareness and educate GYWs on digital safety. In addition, various art-based initiatives, such as ball games, public speaking, and dances, are also used to educate and engage the community. Some organisations have introduced campaigns like “Mental Fridays” and Twitter marathons to offer safe spaces to discuss online safety, mental health, and cyberbullying. Posters, school sensitizations, and online webinars also play a key role in educating both girls and the wider community. Collectively, these initiatives aim to empower GYWs, provide them with tools to navigate the digital world safely, and raise awareness about the dangers of online abuse. However, challenges remain in ensuring that all GYW, especially those in remote areas, have access to these resources.

29 ChildFund International and African Child Policy Forum. (2024, May 30). [Online exploitation and abuse of children in Africa on the rise](#). ChildFund Alliance.

30 ECPAT, INTERPOL and UNICEF. (October, 2021). [Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse](#). Global Partnership to End Violence against Children. 38.

31 Ms Bosibori. (2023, December 13). [Protect Women from Rising Online Gender-Based Violence](#). International Commission of Justice.

32 Agnes Oloo. (2024, April 03). [Tech-fueled Gender-based violence rampant in Kenya’s institutions of higher learning-study](#). Citizen Digital.

33 ECPAT, INTERPOL and UNICEF. (October, 2021). [Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse](#). Global Partnership to End Violence against Children. 72.

34 Ibid, 71.

35 Ibid, 72.

36 Ibid, 71.



LEGAL FRAMEWORK AND LAW ENFORCEMENT RESPONSE

The existing national laws relevant to OSEA-related crimes in Kenya are the Computer Misuse and Cybercrimes Act and the Sexual Offences Act. In 2022, Kenya enacted the Children Bill 2021, criminalising online grooming, but the provision does not consider grooming when the sexual abuse takes place online.³⁷ There is no specific provision criminalising the live-streaming of child sexual abuse and sexual extortion committed in the online environment. Furthermore, no provisions that explicitly recognise the rights and specific needs of girls and young women are included.

The main policy which touches on OCSEA is the National Plan of Action to Tackle Online Child Sexual Exploitation and Abuse in Kenya 2022–2026.³⁸ It provides a strategic framework for preventing and responding to online threats against children. In addition, in 2024, the Ministry of Labour and Social Protection produced the Standard Operating Procedures on Online Child Sexual Exploitation and Abuse in Kenya, a guide for professionals addressing OCSEA.³⁹

Regarding law enforcement response, the Anti-Human Trafficking & Child Protection Unit (AHTCPU) is specialised in addressing OCSEA cases in Kenya. However, it seems that it is difficult to access and report to the unit.⁴⁰ In addition, it appears that regular police units are not obliged to refer cases of OCSEA to the AHTCPU unit. Many police officers may not be aware of the unit's existence.⁴¹ There is a lack of awareness, training and technical knowledge of OCSEA and technology-facilitated gender-based violence among police officers.⁴² The findings from Disrupting Harm revealed that among the young people interviewed about their experiences seeking justice after being victims of OCSEA, some had positive interactions with the police, while most felt let down. For instance, some children reported that they were not informed about their rights or were not questioned in a sensitive manner. Others expressed dissatisfaction with officers who displayed harsh judgments and negative attitudes towards them.⁴³ More generally, there is a lack of trained professionals, equipment, and technical expertise on OCSEA and technology-facilitated gender-based violence.

No information is to be found on cases of girls or young women victims of OCSEA and/or technology-facilitated gender-based violence successfully securing compensation.



37 Kenya gazette Supplement. (2022, July 12). [The Children Act 2022](#). Republic of Kenya.

38 Ministry of Public Service, Gender, Senior Citizens Affairs and Special Programmes State Department for Social Protection, Senior Citizens Affairs and Special Programmes Directorate of Children's Services. (2022). [National Plan of Action to Tackle Online Child Sexual Exploitation and Abuse in Kenya 2022-2026](#). Republic of Kenya.

39 Ministry of Labour and Social Protection, Directorate of Children Services. (2024). [Standard Operating Procedures on Online Child Sexual Exploitation and Abuse in Kenya](#). Republic of Kenya.

40 ECPAT, INTERPOL and UNICEF. (October, 2021). [Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse](#). Global Partnership to End Violence against Children. 73.

41 Ibid, 75.

42 Ibid, 75.

43 Ibid, 8.



LIBERIA

CONTEXT



According to UNICEF, in Liberia, 75% of youth have one or two mobile phones, mobile phones being the main mode of communications,⁴⁴ and 95% of children are using the Internet.⁴⁵ In 2019, DCI-Liberia collaborated with the Internet Watch Foundation Liberia network and opened a reporting portal, where Liberians anonymously and confidentially can report child sexual abuse and exploitation material.⁴⁶ However, reporting mechanisms for OCSEA and technology- facilitated gender-based violence are limited and poorly known in Liberia.

In Liberia, some organisations are actively engaged by proposing Sexual and Reproductive Health Services and Sexual and Gender-Based Violence online series, teaching digital safety practices, running awareness campaigns on radio and social media, and through the 'She Leads' programme.

There is a clear lack of research undertaken and data collected on OSEA and technology- facilitated gender-based violence in Liberia.

LEGAL FRAMEWORK AND LAW ENFORCEMENT RESPONSE

The existing national law relevant to OCSEA-related crimes in Liberia is the Cybercrime Act 2021 which criminalised CSAM and partially grooming.⁴⁷ However, this law doesn't explicitly and fully criminalise all forms of OCSEA-related offences nor include provisions that explicitly recognise the rights and specific needs of girls and young women.

Regarding law enforcement response, there is no specific agency, unit or plan to specifically address OCSEA cases in Liberia nor technology-facilitated gender-based violence.

At all levels, there is a lack of trained professionals, capacity, equipment, and technical expertise on OCSEA and technology-facilitated gender-based violence.

The main barrier to access to justice is the victims' lack of awareness regarding their rights, available remedies, and protective measures. Additionally, many victims face financial constraints and a lack of support, which hinder their ability to pursue claims and seek protection.⁴⁸

No information is to be found on cases of girls or young women victims of OSEA and/or technology-facilitated gender-based violence successfully securing compensation.

44 Defence for Children-Liberia. (2019, October 03). [Sexual Exploitation of Children in Liberia Submission for the Universal Periodic Review of the Human Rights situation in Liberia.](#)

45 Angela Munoz Aroca. (2019, February 15). [Liberia marks Safer Internet Day with crackdown on online child sexual abuse images and videos – supported by UK's IWF.](#) UK Safer Internet Centre.

46 (2019, February 14). [Liberia: Pro-Children Advocacy Group Launches Campaign Against Online Child Abuse Images.](#) Front Page Africa.

47 Republic of Liberia. (2022). [AN ACT TO PROVIDE FOR THE PROHIBITION, PREVENTION, DETECTION, RESPONSE AND PROSECUTION OF CYBERCRIME, TO BE KNOWN AS CYBERCRIME ACT 2021.](#)

48 Global Compendium - Human Trafficking Laws. (2023). [LIBERIA'S LAWS APPLICABLE AS OF JUNE 2021.](#) 22





MALI

CONTEXT



Cyberbullying is a growing phenomenon in Mali, as is the publication of images that compromise the privacy of others, some of which being edited with the intention of damaging the reputation of others.⁴⁹ These phenomena affect women in particular, as some female influencers testify.⁵⁰

In 2020, Internet Watch Foundation launched a new reporting portal in Mali with the collaboration of the government, allowing people in the country to report child sexual abuse material.⁵¹ However, there appears to be a lack of effective channels for both children and adults to report cases of OCSEA and technology-facilitated gender-based violence.

In Mali, only few organisations are actively involved in addressing OCSEA and technology-facilitated gender-based violence targeting girls and young women through projects focusing on raising awareness among young girls of the dangers of social media and training workshops with the local centre, targeting young women, girls and the police. Awareness raising initiatives on OSEA and technology-facilitated gender-based violence include digital campaigns, school-based awareness programs, and discussions on protecting girls' rights and preventing harassment. One organisation has formed a WhatsApp group for participants to share ideas, information, and conduct local awareness sessions after attending training.

There is a real lack of research and data collection on OSEA and technology-facilitated gender-based violence in Mali.

LEGAL FRAMEWORK AND LAW ENFORCEMENT RESPONSE

In 2019, Mali adopted Law No. 2019-056 on the repression of cybercrimes.⁵² In relation to crimes related to OCSEA and technology-facilitated gender-based violence, the law defines and criminalises the offence of disseminating CSAM and cyberbullying partially.⁵³ However, it doesn't explicitly and fully criminalise all forms of OCSEA-related offences nor include provisions that explicitly recognise the rights and specific needs of girls and young women.

In 2015, the Malian government established the Personal Data Protection Authority (ADPD), which is responsible for protecting individuals with regard to the processing of personal data. The ADPD receives complaints and refers offences to the competent public prosecutor. In 2013, the APDP expressed its deep concern about the misuse of social networks in general, and TikTok in particular, by women and minors.⁵⁴ In 2022, the government adopted a new regulation creating a specialised judicial unit to combat cybercrimes.⁵⁵ However, there does not seem to be a specific unit to deal with cases relating to OCSEA and technology-facilitated gender-based violence.⁵⁶

At all levels, there is a critical lack of trained professionals, capacity, equipment and technical expertise in online child sexual exploitation and gender-based violence in Mali. Justice remains legally, economically and socially inaccessible for survivors. There are three criminal courts throughout Mali, one in Mopti covering the regions of Ménaka, Kidal, Gao, Mopti and Timbuktu, one in Bamako covering all the regions of Bamako, Ségou and Sikasso and one in Kayes covering the region of Kayes. So, for example, a victim

49 Le Pays. (2019, January 14). [Développement numérique au Mali : Les réseaux sociaux, antichambre d'un dérapage éducatif](#). Maliweb.

50 Abdoul Salam DICKO. (2024, July 31). [Cyberharcèlement : le cauchemar des influenceuses au Mali](#). Benbere

51 Internet Watch Foundation. (2020, May 07). [Tech companies and charities unite to keep children in Mali safe online](#).

52 République du Mali. (2019, Décembre 13). [Journal Officiel de la République du Mali](#).

53 Cheibane Dembele. (2024, August 31). [Cyberharcèlement : les sanctions prévues par la loi sur la cybercriminalité au Mali](#). Benbere.

54 Ismaila Traore. (2023, April 14). [Communiqué de presse](#). ADPD.

55 République du Mali. (2019, Décembre 13). [Journal Officiel de la République du Mali](#).

56 ECPAT France, ECPAT Luxembourg et ECPAT International. (2017). [Rapport Global de Suivi de la Mise en Oeuvre des Actions de Lutte contre l'Exploitation Sexuelle des Enfants à des fins commerciales](#). 36



in a village in Timbuktu who wants to obtain justice has to face enormous financial costs. No information is to be found on cases of girls or young women victims of OCSEA and/or technology-facilitated gender-based violence successfully securing compensation.



SIERRA LEONE

CONTEXT



Cases of OCSEA and technology-facilitated gender-based violence are occurring in Sierra Leone. A 2022 report by ChildFund International revealed that approximately 20% of girls aged 15-19 in Sierra Leone have experienced online sexual exploitation or abuse. Similarly, a 2021 study by the Sierra Leone Ministry of Education found that 24% of teenagers have been victims of cyberbullying. Additionally, a survey conducted by the Sierra Leone Cyber Security Authority in the same year indicated that 17% of young women have been affected by various forms of cybercrime. According to the Media Foundation for West Africa, Women and girls are disproportionately targeted by online harassment and abuse, including cyberbullying, revenge porn, and stalking in Sierra Leone. This has severely affected their safety, well-being, and participation in public life and limited their opportunities for civic engagement and political participation.⁵⁷ Finally, a report from a social change website indicates that over 43% of young people surveyed have experienced online bullying. The most common medium for cyberbullying is mobile smartphones, and girls and young women are more than twice as likely as boys to be both victims and perpetrators of cyberbullying.⁵⁸

In 2020, Internet Watch Foundation launched a new reporting portal in Sierra Leone with the collaboration of the government of Sierra Leone, allowing people in the country to report child sexual abuse material.⁵⁹ Other reporting channels also exist, such as the Cybercrime Unit of the Sierra Leone Police, the Family Support Unit, the Human Rights Commission, and Independent Media Commission. Additionally, some regions have hotlines (e.g., 116) or toll-free services.

In 2023, The African Committee of Experts on the Rights and Welfare of the Child stated that the government of Sierra Leone needed to take immediate action to the emerging challenge of online child sexual exploitation and abuse.⁶⁰

Some organisations are actively involved in the fight against OCSEA and technology-facilitated gender-based violence by taking initiatives ranging from capacity-building training, community sensitisation, awareness campaigns, legal and psychological support, advocacy, and the establishment of safe spaces for young women. Regarding awareness-raising, activities include radio discussions, social media campaigns, school workshops, community outreach, and collaborations with local authorities. These efforts focus on educating girls and young women on cyber safety, digital citizenship, and how to report cyberbullying.

There is a clear lack of research undertaken and data collected on OCSEA and technology-facilitated gender-based violence in Sierra Leone.

LEGAL FRAMEWORK AND LAW ENFORCEMENT RESPONSE

The existing national laws relevant to OCSEA-related crimes in Sierra Leone are the Child Rights Act, the Sexual Offences Act 2019, and the Cybersecurity and Crime Act 2021. However, those laws don't explicitly and fully criminalise all forms of OCSEA-related offences nor include provisions that explicitly recognise the rights and specific needs of girls and young women.

57 Media Foundation for West Africa, Embassy of the Kingdom of the Netherlands in Ghana. (2023, August). [Women's Rights Online in Sierra Leone: Policy Gaps and Recommendations for Promoting Gender Equality and Empowerment](#). 3.

58 Humphrina Pearce. (2023, Decembre 8). [The state of Cyber-Bullying in Sierra Leone: Where is the law?](#). Sierra Lii.

59 Internet Watch Foundation. (2020, January 30). ['Unprecedented collaboration' will help fight against online child sexual abuse](#).

60 ACERWC. (2023, August 11). [The African Committee of Experts on the Rights and Welfare of the Child has just concluded its follow-up mission in the Republic of Sierra Leone](#).



In 2021, the Ministry of Information and Communications launched the National Cybersecurity Policy which briefly mentions the promotion of online child protection.⁶¹

The National Cybersecurity Coordination Centre (NC3) was established in 2021. While its primary focus is not exclusively on OCSEA, it is an integral part of its mandate. For instance, in 2024, the NC3 launched its School Outreach initiative, designed to engage students in discussions about digital safety, raise awareness about the importance of cybersecurity, and empower them to contribute to creating a safer online environment.⁶²

In 2023, The Ministry of Basic and Senior Secondary Education developed the Comprehensive School Safety Policy which includes guidelines on protecting students from unsafe, dangerous, or risky online situations and behaviours, and develop positive online behaviour in students.

Despite some progress, there is a lack of trained professionals, equipment, and technical expertise on OCSEA and technology-facilitated gender-based violence.⁶³

No information is to be found on cases of girls or young women victims of OCSEA and/or technology-facilitated gender-based violence successfully securing compensation.



61 Ministry of Information and Communications. (2021, March). [National Cybersecurity Policy](#). Government of Sierra Leone.

62 National Cybersecurity Coordination Centre. (2024, February 01). [NC3 School Outreach Initiative](#).

63 Mohamed Wurie Bah. (2023, November 24). [Sierra Leone's Cybersecurity Odyssey: Progress, challenges, and future paths](#). Institute for Legal Research and Advocacy for Justice.

UGANDA

CONTEXT



As demonstrated by the Disrupting Harm research, children in Uganda are subjected to OCSEA. OCSEA mostly occurs on social media such as Facebook Messenger and WhatsApp.⁶⁴ Cases of OCSEA included unwanted requests for children to talk about sex and unwanted requests for images showing their private parts as well as being offered gifts in return for sexual images and being threatened or blackmailed online to engage in sexual activities.⁶⁵ Most children who experienced potential grooming attempts resisted the requests, although a small percentage complied with unwanted demands. Ten percent of internet-using children aged 15 to 17 reported accepting money or gifts in exchange for sexual images or videos. Additionally, nine percent stated that sexual images of them had been shared without their consent in the past year.⁶⁶ In Uganda, girls made up over 98% of the victims of all recorded sex offences against juveniles in 2017–2019.⁶⁷ According to the Disrupting Harm findings, slightly more girls than boys reported receiving unwanted requests for a photo or video showing their private parts.⁶⁸ In addition, girls were more likely to be subjected to sexual comments about them that made them feel uncomfortable – including jokes, stories or comments about the child’s body, appearance or sexual activities.⁶⁹

Public awareness and understanding of OSEA are low. OSEA and technology-facilitated gender-based violence are considered as new issues for many citizens in Uganda. Law enforcement officers, criminal justice professionals and frontline workers also lack awareness of OCSEA and technology-facilitated gender-based violence.⁷⁰

However, some organisations raise-awareness through activities such as online Twitter chats and spaces to discuss cybercrime, mentorship programs in schools to educate students on the different forms of cybercrimes and online violences, and weekly sessions on mental health. Other organisations focus on identifying gaps in online child sexual exploitation and abuse legislation and its implementation, initiating and carrying out appropriate responses as well as advocating for care facilities with trained staff who can recognize and respond to victims of OCSEA and technology-facilitated gender-based violence.

The majority of cases of OSEA and technology-facilitated gender-based violence are not officially reported in Uganda. There seems to be a lack of channels through which children and adults can report cases of OCSEA and technology-facilitated gender-based violence. Children lack familiarity with reporting mechanisms on social media platforms they use, helplines and the police, or do not perceive OCSEA and technology-facilitated gender-based violence as wrong or important enough.⁷¹

There is a lack of research undertaken and data collected on OCSEA and technology-facilitated gender-based violence in Uganda.

LEGAL FRAMEWORK AND LAW ENFORCEMENT RESPONSE

The existing national laws relevant to OCSEA-related crimes in Uganda are the Penal Code Act, the Computer Misuse Act (2011), the former AntiPornography Act, and the Children Act. There is no specific provision criminalising the livestreaming of child sexual abuse, prohibiting online grooming for sexual purposes and sexual extortion committed in the online environment, nor incorporate gender perspectives

64 ECPAT, INTERPOL and UNICEF. (2021). [Disrupting Harm in Uganda: Evidence on online child sexual exploitation and abuse](#). Global Partnership to End Violence against Children. 46.

65 Ibid, 6.

66 Ibid, 6.

67 Ibid, 63.

68 Ibid, 48.

69 Ibid, 59.

70 Ibid, 69.

71 Ibid, 66.



to include provisions that explicitly recognise the rights and specific needs of girls and young women. Regarding law enforcement response, there is no specific unit or plan addressing OCSEA cases in Uganda. The Directorate of Criminal Investigations is responsible for the investigation of all crimes in the country, and the Sexual and Gender-Based Violence Unit investigates many of the OCSEA-related crime cases. There is no disaggregated data specifically about the outcomes of OCSEA investigations. At all levels, there is a lack of trained professionals, equipment, and technical expertise on OCSEA and technology-facilitated gender-based violence.⁷² The six Ugandan OCSEA victims in the access to justice interviews in the Disrupting Harm research, all girls, consistently characterised their encounters with most local officials and police in negative, and even painful, terms. With few exceptions, they said that the police and local councillors were not genuinely motivated to help them pursue justice.⁷³

No information is to be found on cases of girls or young women victims of OSEA and/or technology-facilitated gender-based violence successfully securing compensation.



72 Ibid, 78.

73 Ibid, 81.



DATA ON THE PREVALENCE, EXPERIENCES, AND IMPACTS OF OSEA AND TECHNOLOGY-FACILITATED GBV IN SOUTHERN AFRICA

Similar trends across the Southern African countries (Zambia, Malawi, Zimbabwe, Angola, Botswana, Namibia and Mozambique) pinpoint the occurrence, and severe effects and impacts of technology-facilitated gender-based violence against girls and young women. A rise in the cases has been noted, especially with the increase in access to Information and Communication Technologies (ICT) in Africa and the low levels of awareness of risks associated with accessing online platforms.

The issue of technology-facilitated gender-based violence remains largely underreported. The lack of a centralised database in countries makes it difficult to accurately assess the full extent of technology-facilitated gender-based violence. Furthermore, these cases are rarely reported due to factors such as cultural traditions and social stigma, inadequate application of the law, limited reporting mechanisms and lack of awareness of available reporting procedures and mechanisms. Finally, minimal disaggregation of data related to this issue, further complicating efforts to understand its scope.

Although some laws have been enacted, most existing laws and policies do not explicitly and fully criminalise all forms of technology-facilitated gender-based violence. Moreover, some laws are outdated and contain provisions that can be used against the victims themselves.

Women and girls, particularly those with disabilities or in leadership roles, face a higher risk of technology-facilitated gender-based violence. The impact of these violations is often severe and can be life-altering, significantly threatening the well-being of victims, with consequences that extend across borders.



ANALYSIS OF THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION MALABO CONVENTION⁷⁴

The African Union Convention on Cyber Security and Personal Data Protection provides a crucial legal framework aimed at enhancing cybersecurity and safeguarding personal data across member states. It covers a wide range of topics, including legal and institutional frameworks, cooperation mechanisms, and data protection. However, while the convention addresses critical issues such as cybercrime and human rights violations in cyberspace, it does not explicitly target the specific challenges faced by girls and young women, particularly in relation to online sexual exploitation and abuse, cybercrime and cyberbullying. Although the convention's focus on combating cybercrime is a positive step toward addressing some of these issues, it overlooks the intersection of gender and cybersecurity. For example, the Girls and Young Women noticed a gap in provisions related to online harassment, privacy violations, and the digital literacy needs. Additionally, the convention does not mandate the collection or reporting of gender-disaggregated data on cybersecurity and personal data protection, which is vital for understanding and addressing the unique vulnerabilities of women and girls in the digital space. While the convention provides a foundational framework for legislative modernisation and the protection of personal data, its success will depend on the ability of member states to implement these rules effectively, particularly in diverse cultural, legal, and socio-economic contexts. The convention also emphasises international cooperation to combat cybercrime and human rights violations globally, highlighting the need for regional coordination and harmonisation of legislative measures. However, for it to be truly effective in addressing technology-facilitated gender-based violence, member states must go beyond the general provisions and ensure that the voices, rights, and needs of girls and young women are incorporated into these efforts.

The African Union Convention on Cyber Security and Personal Data Protection lays the groundwork for improving cybersecurity and data protection, but it must be strengthened by a more inclusive approach that specifically addresses the challenges faced by girls and women. By integrating gender perspectives and promoting gender-disaggregated data collection, member states can better respond to the digital vulnerabilities of girls and young women, fostering a safer and more equitable digital environment for all.

While the Malabo Convention has the potential to play a crucial role in addressing cybercrime, and technology-facilitated gender-based violence regionally, its impact is often limited by the lack of ratification and local adaptation in countries.⁷⁵ With countries ratifying and domesticating the Convention, integrating it with country-specific interventions, it could serve as a strong foundation for policy development and enforcement at the national level. The process of localisation would enable more effective responses, particularly for girls and young women facing OCSEA and technology-facilitated gender-based violence.

⁷⁴ [African Union Convention on Cyber Security and Personal Data Protection](#) (Malabo Convention), adopted on June 27, 2014.

⁷⁵ To date, of the seven She Leads Programme implementing countries where girls and young women have conducted the assessment on Online Sexual Exploitation and Abuse and Tech-facilitated Gender Based Violence only Ghana has ratified the Malabo convention, with Sierra Leone having signed it without yet ratifying.





The African Women's
Development and
Communication Network

Girls & Young Women-Led Assessment on Online Sexual Exploitation, Abuse & Technology-Facilitated Gender-Based Violence in Africa

