
INTERNATIONAL JOURNAL OF SCIENCE ARTS AND COMMERCE

EXAMINING THE LEGAL FRAME FOR PROTECTING CHILDREN FROM ONLINE SEXUAL EXPLOITATION AND ABUSE IN TANZANIA

Ramadhani Kitwana Jongo

Senior Legal Officer

Ministry of Communication and Information Technology ,

P.O.Box 677, Government City, Mtumba Area,

9 Mawasiliano Street,

40470 Dodoma.

**CANDIDATE IN MASTER OF LAWS IN ICT AND TELECOMMUNICATION (LLM
LAM) OF THE OPEN UNIVERSITY OF TANZANIA**

ABSTRACT

Tanzania, like many African nations, grapples with systemic challenges in aligning its legal frameworks with emerging digital threats. Each time children access social media or instant messaging platforms, they are susceptible to online sexual exploitation and abuse, as well as other forms of peer-to-peer violence. This has created unprecedented opportunities for children to communicate, learn, socialize and play, exposing them to new ideas and more diverse sources of information. This study examines the legal framework for protection children from online sexual exploitation and abuse in Tanzania. A researcher employed Qualitative Legal Approach grounded in doctrinal, comparative and empirical research methods, the study assesses the sufficiency of Tanzania's domestic law and Institutional enforcement mechanism in protecting child from sexual exploitation and abuse in Tanzania. The findings reveal persistent gaps, including unclear statutory definitions and legal framework is still not entirely sufficient in addressing all types of OCSEA, especially emerging forms like online grooming, live-streaming of abuse in real-time, sexual extortion, and non-contact online coercion. There are also major gaps in implementation, capacity, and regulation. In light of these shortcomings in the legal system for protecting children online. The study concludes that Tanzania should strengthen its legal framework by amending the Child Act and Cybercrime Act; developing and adopt a national policy on online child sexual exploitation and abuse; improving the capacity of law

enforcement, prosecutors, and digital forensic services to investigate online offenses; and raising awareness among children, parents, caregivers, educators, and the public about online risks, how to report abuse, and how online and offline abuse are connected.

Keyword: *Online Child Protection from sexual exploitation and abuse in Tanzania.*

1.1 Introduction

The digital revolution has profoundly altered the life of childhood experience, but the spread of the internet has also heightened risks of online sexual exploitation and abuse (OSEA) of children, necessitating strong legal safeguards.¹ In Tanzania, where the internet penetration grew from 7% in 2011 to 35% in 2024, children are exposed to increasingly increasing risks such as grooming, sextortion, and unsolicited image sharing. Despite legal reforms such as the Cybercrimes Act, Cap 443, the Child Protection Laws (Miscellaneous Amendments) Bill, 2024, there remain systemic gaps in matching domestic frameworks to international standards and responding to emerging digital harms.² Globally, treaties like the UN Convention on the Rights of the Child (UNCRC)³ and the African Charter on the Rights and Welfare of the Child (ACRWC) obligates states to protect children against exploitation, but are weakly implemented.⁴ This study critically evaluates Tanzania child protection law, its adequacy in the face of international norms, and areas of deficiency in enforcement, international collaboration, and support to victims. By synthesizing legal analysis and empirical data, the research aims to propose actionable reforms to enhance Tanzania's capacity to safeguard children in the digital age, contributing to regional and global efforts to combat OSEA.

2.1 International and Regional Legal Frameworks for the Protection of Children from Online Sexual Exploitation and Abuse

2.1.1 The UN Convention on the Rights of the Child (UNCRC) and the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography which has been replaced internationally by " CSAM (OPSC)

The United Nations Convention on the Rights of the Child (UNCRC), adopted in 1989 and ratified by Tanzania in 1991, is the most comprehensive and universally accepted international treaty on children's rights. The UNCRC establishes the foundation of international children's

¹ Odudu, Q. "Child Abuse: The Emerging Role of The Internet And Technology." (2024).

² Tanzania Communications Regulatory Authority, Quarterly Communications Statistics Report (March 2024).

³ United Nations Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.

⁴ African Charter on the Rights and Welfare of the Child (adopted 11 July 1990, entered into force 29 November 1999) OAU Doc CAB/LEG/24.9/49.

rights law by recognizing every child's right to protection from all forms of abuse, exploitation, and violence. Articles 16, 19, 34, 35 and 36 establish comprehensive framework for protecting children from OCSEA. The Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography which been replaced internationally by "CSAM" strengthens these protections by requiring States to criminalize specific forms of child sexual exploitation and enhance international cooperation.⁵

Although these provisions were adopted before the digital age, their broad and rights-based language has enabled them to remain relevant to contemporary forms of online abuse. Nevertheless, significant implementation challenges persist, including inconsistent domestic legislation, limited investigative capacity, jurisdictional conflicts, technological developments, and balancing child protection with privacy and freedom of expression. These challenges demonstrate the need for dynamic interpretation of the Convention alongside newer international instruments and evolving international standards on children's rights in the digital environment.

In the context of OCSEA, violations of privacy frequently occur when offenders obtain, create, distribute, or threaten to distribute intimate images of children without their consent. Offenders may also engage in online grooming by collecting personal information to manipulate children into producing sexually explicit material. Similarly, practices such as sextortion involve coercing children through threats to disclose private images unless further sexual content or acts are provided.

Article 16 therefore, requires States to enact legal and technological safeguards protecting children's digital privacy, regulate the collection and processing of children's personal data, strengthen cybersecurity measures, and ensure that victims have effective remedies when their privacy has been violated.⁶ It also places responsibilities on digital platforms to implement privacy-by-design measures and robust protections for child users.

Article 19 establishes one of the broadest protection obligations within the Convention. It requires governments to develop comprehensive child protection systems incorporating prevention, reporting mechanisms, investigation, treatment, and follow-up services.⁷ Its relevance to OCSEA is extensive. Online grooming, livestreamed sexual abuse, production and distribution of CSAM, cyber-enabled trafficking, and online coercion all constitute forms of sexual abuse falling within Article 19. States must therefore, implement criminal legislation, online safety policies, awareness campaigns, child-friendly reporting mechanisms, specialized investigative units, and multidisciplinary support services. It also emphasizes prevention,

⁵ The UN Convention on the Right of the Child, 1989, Article 16, 19, 34, 35

⁶ Ibid, Article 16

⁷ Ibid, Article 19

requiring governments to educate children, parents, teachers, and communities about online risks while strengthening digital literacy and internet safety programs.

Article 34 specifically addresses sexual exploitation and abuse by requiring States to protect children from: unlawful sexual activity; exploitation in prostitution or other unlawful sexual practices; and exploitation in pornographic performances and materials.⁸ This provision forms the principal legal foundation within the UNCRC for combating child sexual exploitation. Although drafted before the digital era, Article 34 applies equally to online forms of abuse, including online grooming, livestreamed abuse, child sexual abuse material, and sexual exploitation facilitated through digital communication technologies.

The Article requires States to criminalize sexual offences against children, strengthen law enforcement capacity, cooperate internationally, and establish preventive measures. It also supports obligations to investigate internet-based offences involving cross-border criminal networks. Nevertheless, Article 34 uses terminology such as "child pornography," which has increasingly been replaced internationally by "CSAM". The newer terminology recognizes that such material documents abuse rather than pornography involving consenting participants. This linguistic evolution reflects a more victim-centered understanding of exploitation.

Article 35 recognizes that child trafficking frequently transcends national borders and therefore requires international cooperation.⁹ In relation to OCSEA, trafficking increasingly occurs through digital technologies. Criminal networks use social media, encrypted messaging applications, online advertisements, and digital payment systems to recruit, exploit, transport, advertise, and control child victims. Online platforms may facilitate trafficking for sexual exploitation, including livestreamed abuse and commercial production of CSAM.

Implementation of Article 35 therefore, requires States to strengthen cross-border investigations, harmonize criminal legislation, improve information sharing, regulate financial technologies used to facilitate exploitation, and cooperate with internet service providers and digital platforms. Practical implementation remains challenging because trafficking networks frequently operate across multiple jurisdictions with differing legal standards and investigative capacities.

Article 36 functions as a broad residual protection provision by covering exploitative conduct not expressly addressed elsewhere in the Convention. Its open-ended wording enables the Convention to respond to emerging forms of exploitation resulting from technological and social developments. This flexibility is particularly valuable for addressing OCSEA because new forms of online exploitation continue to evolve. These include artificial intelligence-generated child sexual abuse material, deep fake sexual images involving children, sextortion, online sexual

⁸ The UN Convention on the Right of the Child, 1989, Article 34

⁹ Ibid, Article 35

coercion, abuse occurring within virtual environments, exploitation through gaming platforms, and offences involving cryptocurrencies.

The broad language of Article 36 allows States to interpret the Convention dynamically, ensuring that children's rights remain protected despite rapid technological innovation.¹⁰ It complements Articles 19 and 34 by capturing exploitative practices that may not fit traditional legal categories. However, the provision's general wording also creates uncertainty regarding the precise scope of State obligations.¹¹ Effective implementation therefore depends upon domestic legislation clearly defining emerging offences and ensuring that criminal laws remain technologically neutral while adequately protecting children.

Also Article 39 imposes a proactive duty on States to establish systems that facilitate children's recovery. Recovery extends beyond medical treatment to include psychological counselling, trauma-informed care, educational support, family reunification where appropriate, legal assistance, and social services.¹² The provision recognizes that child victims frequently experience long-term trauma, including anxiety, depression, post-traumatic stress disorder (PTSD), shame, social isolation, and difficulties in trusting others.

In OCSEA cases, recovery presents unique challenges because digital abuse often has enduring consequences. Images or videos depicting abuse may remain online indefinitely, be repeatedly shared across jurisdictions, and resurface years after the initial offence. As a result, victims may experience repeated psychological harm arising from the fear that the abuse is continually being viewed or redistributed. Consequently, recovery under Article 39 requires long-term and specialized mental health support rather than short-term intervention.

The Convention requires governments to adopt legislative, administrative, educational, and social measures to protect children, thereby encouraging holistic responses that include prevention, rehabilitation, and child participation. However, significant legal limitations exist. Consequently, it contains no explicit provisions addressing cyber-enabled offences such as online grooming, livestreamed child sexual abuse, sextortion, artificial intelligence-generated child sexual abuse material, or encrypted communications used by offenders. Although the Optional Protocol criminalizes child pornography, its terminology now preferred concept of CSAM, which better reflects the abusive nature of the content and avoids implying legality or consent.

¹⁰ Ibid, Article 36

¹¹ Ibid, Article 19, 34

¹² Ibid, Article 39

Tanzania ratified the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, its terminology now preferred concept of CSAM in 2003. The OPSC strengthens the obligations under Article 34 by requiring states to criminalize, prevent, and prosecute the sale of children, child prostitution, and child pornography in all forms, including digital. Article 3 of the Protocol mandates that states criminalize the production, distribution, dissemination, importation, exportation, offering, and possession of CSAM.¹³

Despite these ratifications, Tanzania's domestic legal alignment remains fragmented. As analyzed in earlier sections, national laws like the Cybercrimes Act, Cap 443 and the Law of the Child Act, Cap 13 fall short of fully incorporating the obligations under the CRC and OPSC. For instance, there is no clear legal definition of grooming or livestreaming of child abuse, and enforcement agencies lack structured procedures for handling digital evidence involving child victims. Moreover, national laws do not explicitly refer to the best interests of the child in digital investigations or prosecutions as required under Article 3 of the UNCRC.

These gaps highlight the disconnect between Tanzania's treaty obligations and its legislative and enforcement frameworks, reinforcing the need for reform. Effective implementation of these instruments requires not only legal reform but also cross-sectoral cooperation, digital literacy training for law enforcement and judicial officers, and the creation of child-friendly procedures for reporting and investigating online exploitation.

2.1.2 African Charter on the Rights and Welfare of the Child (ACRWC)

The African Charter on the Rights and Welfare of the Child (ACRWC), adopted by the Organization of African Unity (now African Union) in 1990 and entered into force in 1999, is a binding regional instrument designed to protect and promote the rights and welfare of children in Africa.¹⁴ The African Charter on the Rights and Welfare of the Child provides Africa's regional framework for child protection. It reflects many principles contained in the UNCRC while addressing African social, cultural, and developmental contexts. Articles 16, 21, 27, and 29 prohibit child abuse, harmful practices, sexual exploitation, trafficking, and sale of children¹⁵.

But its principal strength lies in contextualizing children's rights within African realities. It addresses issues such as child marriage, harmful traditional practices, armed conflict, and socioeconomic vulnerability, all of which increase children's susceptibility to online exploitation. The Charter also places significant emphasis on State responsibility and community involvement in child protection. Despite these strengths, the Charter has notable weaknesses regarding OCSEA. Similar to the UNCRC, it predates the digital era and therefore contains no explicit

¹³ Optional Protocol to the Convention on the Rights of the Child, Article 3

¹⁴ African Charter on the Rights and Welfare of the Child, (adopted 11 July 1990, entered into force 29 November 1999) OAU Doc CAB/LEG/24.9/49 (1990).

¹⁵ Ibid, ss 16, 21, 27, 29.

provisions dealing with cyber enabled child sexual abuse. Emerging forms of exploitation including online grooming, sexual sextortion, livestreaming of abuse, cryptocurrency facilitated exploitation, and abuse occurring through gaming platforms or social media are not specifically addressed.

Implementation remains irregular across African States. Many countries face resource constraints, limited cybercrime investigative capacity, shortages of trained digital forensic experts, and inadequate child protection systems. Legislative harmonization across African jurisdictions also remains incomplete, creating obstacles for cross-border investigations and extradition.

Institutionally, the African Committee of Experts on the Rights and Welfare of the Child has relatively limited enforcement powers. While it can monitor implementation and receive communications, compliance largely depends upon political commitment by Member States. Consequently, significant gaps persist between legal obligations and practical enforcement. Tanzania ratified the Charter in 2003, thus assuming legal obligations to incorporate its principles into domestic law and ensure that children are protected from all forms of abuse, including OCSEA.

The Charter establishes broad protections for children's rights across civil, political, economic, social, and cultural dimensions. Notably, Article 16 obliges state parties to protect children from all forms of child abuse, torture, inhuman or degrading treatment, or neglect. This broad obligation extends to the digital sphere, where online grooming, sextortion, and the dissemination of child sexual abuse material represent modern manifestations of exploitation that threaten children's dignity and safety.¹⁶

Further, Article 27 of the Charter calls on state parties to protect children from sexual exploitation and abuse, particularly the use of children in prostitution or pornography. This provision is crucial in the context of OCSEA, as it mirrors the requirements under international law, particularly the UNCRC Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, while contextualizing the problem within African sociocultural settings.¹⁷

The ACRWC is distinctive in its regional orientation and emphasis on collective cultural and communal values, which can support more contextually appropriate policy interventions in countries like Tanzania. Its framework also addresses the need for special measures for vulnerable groups of children, such as those with disabilities or those living in rural areas who may be exposed to online risks due to digital illiteracy or lack of parental supervision.

¹⁶ Ibid, Article 16

¹⁷ Ibid, Article 27

However, despite its binding nature, the ACRWC does not include explicit language around digital technologies, cyberspace, or internet-facilitated crimes, largely because it was drafted before the internet became a widespread societal tool. This necessitates interpretive expansions and legislative adaptations to ensure that domestic legal systems, like Tanzania's, apply these protections in the online environment.

Tanzania's alignment with the ACRWC remains partial in practice. While the country has ratified the Charter and incorporated some of its provisions in laws like the Law of the Child Act (2009), gaps remain, especially in terms of enforcement mechanisms and comprehensive legal coverage of OCSEA. There are no explicit statutory interpretations or regulations under Tanzanian law that align Article 27 with online child protection.¹⁸ This illustrates the implementation gap between ratification and practical enforcement, necessitating stronger domestic laws that align with the Charter's intent.

2.1.3 Malabo Convention (AU Convention on Cybersecurity and Personal Data Protection)

The African Union Convention on Cyber Security and Personal Data Protection, commonly referred to as the Malabo Convention, was adopted on 27 June 2014 in Malabo, Equatorial Guinea. This Convention serves as a continental framework for the harmonization of cybersecurity and data protection laws across Africa. It reflects the growing recognition by African states of the need to address emerging threats in the digital sphere, including OCSEA, through coordinated legal standards and institutional frameworks.¹⁹

The Malabo Convention provides a binding legal instrument, aiming to promote cybersecurity, combat cybercrime, and protect personal data and privacy within African Union (AU) member states. It represents Africa's principal regional instrument addressing cybersecurity, cybercrime, electronic commerce, and data protection. Not drafted specifically to combat OCSEA, its cybercrime provisions create an important legal foundation for investigating and prosecuting offences committed through digital technologies.

The Convention's major contribution lies in encouraging African States to modernize cybercrime legislation and strengthen international cooperation. It promotes criminalization of computer-related offences, procedural powers for digital investigations, electronic evidence collection, and cybersecurity governance. These measures indirectly enhance States' capacity to combat OCSEA.

¹⁸ Ibid, Article 27

¹⁹ African Union, Convention on Cyber Security and Personal Data Protection (Malabo Convention) (adopted 27 June 2014). <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 16 September 2025.

Also the Convention's established regional principles governing personal data protection. It requires States to adopt legal frameworks regulating the collection, processing, storage, and transfer of personal data while recognizing privacy as a fundamental right. These provisions are particularly important in relation to children. Offenders engaged in OCSEA frequently obtain children's personal information through social media profiles, online games, educational platforms, or phishing schemes. Such information may be used to identify vulnerable children, facilitate online grooming, impersonate trusted individuals, or commit sextortion and other forms of sexual exploitation.

By requiring lawful and secure processing of personal data, the Convention contributes to reducing children's exposure to these risks. Strong data protection obligations can limit unnecessary collection of children's information, require appropriate security safeguards, and reduce opportunities for unauthorized access or disclosure. Data protection authorities established under national legislation can also play an important role in ensuring that organizations handling children's personal information comply with privacy standards. Nevertheless, the Convention does not contain provisions specifically recognizing children's heightened vulnerability in the digital environment. It lacks detailed rules on children's consent to data processing, profiling of minors, behavioral advertising directed at children, or the enhanced safeguards recommended in more recent international standards. Consequently, while the Convention strengthens privacy protection generally, additional child-specific legislative measures remain necessary.

The investigation and prosecution of OCSEA offences depend heavily on access to digital evidence. Electronic communications, internet protocol (IP) addresses, subscriber information, metadata, and transaction records are often essential for identifying offenders, locating victims, and reconstructing criminal activity. The Malabo Convention supports the development of national legal frameworks that enable competent authorities to investigate cybercrime and obtain electronic evidence in accordance with domestic law. Appropriate data retention obligations can assist law enforcement agencies by ensuring that relevant information remains available long enough to support criminal investigations and prosecutions.

In OCSEA cases, preservation of electronic evidence is especially important because offenders frequently delete files, use encrypted communication services, or operate across multiple jurisdictions. Retained data may enable investigators to identify offenders involved in online grooming, distribution of CSAM, or livestreamed sexual abuse.

The Convention's broad provisions are instrumental in creating enabling environments for digital child protection. For example, Article 111 focuses on establishing effective cybersecurity governance and cybercrime legislation among member states, encouraging them to adopt and enforce national laws criminalizing acts such as illegal data access, data breaches, and online

exploitation, all of which are relevant in prosecuting OCSEA cases.²⁰ Further, Chapter II of the Convention, titled “Fundamental Principles Applicable to the Processing of Personal Data”, places special emphasis on safeguarding individuals’ personal data, including that of minors. The protection of children’s digital privacy is a crucial aspect in combatting OCSEA, as predators often collect and misuse children’s data for grooming or blackmail. The Convention requires state parties to ensure that digital service providers and data processors take adequate steps to safeguard personal information, implement cybersecurity controls, and enable lawful investigation and prosecution of cyber offences.

Tanzania signed the Malabo Convention on 23 February 2023, becoming one of the few countries in the East African region to take steps toward legal harmonization with AU standards. However, as of July, 2026, Tanzania has not yet ratified the Convention, which limits its binding effect and implementation in the domestic legal framework. The delay in ratification reflects broader regional hesitations around data governance, cross-border cyber law enforcement, and institutional readiness.²¹

The Malabo Convention’s relevance to OCSEA lies in its call for national legislation that reflects both technological realities and human rights protections. Although not child-specific, it fills an important normative gap by offering legal templates and guiding principles that can be adapted into national laws to include child-specific cyber protections, such as obligations on internet service providers (ISPs), reporting mechanisms, and digital evidence management.²²

Its potential to bridge enforcement gaps in Tanzania is significant. Ratifying and domesticating the Malabo Convention would obligate Tanzania to reform laws such as the Cybercrimes Act ,2015 and the Electronic and Postal Communications (Online Content) Regulations, 2020 to include OCSEA-specific provisions and to strengthen cross-border investigative cooperation, which is currently a major challenge due to jurisdictional constraints.

2.1.4 Budapest Convention on Cybercrime

The Convention on Cybercrime of the Council of Europe, commonly referred to as the Budapest Convention, was adopted on 23 November 2001 in Budapest, Hungary. It remains the first and most comprehensive international treaty that addresses crimes committed via the internet and other computer networks. The Convention serves to harmonize national laws, improve

²⁰ Ibid, Article 111

²¹ Akongburo, Raymond Atuguba, Patricia Boshe, Sena Afua Dei-Tutu, and Moritz Hennemann, eds. *African Data Protection Laws: Regulation, Policy, and Practice*. Vol. 3. Walter de Gruyter GmbH & Co KG, 2024.

²² The Malabo Convention

investigative techniques, and facilitate international cooperation, making it a critical legal instrument in fighting OCSEA.²³

The Convention includes substantive criminal law provisions targeting offenses against and by means of computer systems. These include the distribution of child pornography which has increasingly been replaced internationally by "CSAM under Article 9, illegal access to computer systems under Article 2, data and system interference under Articles 4 and 5, and offenses related to computer content as provided under Article 10. While it predates some newer forms of OCSEA such as livestreaming and grooming via encrypted messaging apps, its flexibility has allowed it to remain relevant in guiding countries on adapting their laws to current technological threats.²⁴

Article 9 of the Convention is particularly relevant to OCSEA. It requires state parties to criminalize the production, possession, and distribution of child pornography through computer systems. It also outlines that "child" refers to any person under 18 years, and mandates that member states criminalize acts involving simulated sexual conduct, non-visual content, and any material that depicts a child in sexually explicit conduct. This broad definition is crucial in ensuring comprehensive coverage of the different forms of CSAM encountered online.²⁵

Despite its global relevance and adoption by over 70 countries, Tanzania is not a party to the Budapest Convention. This lack of ratification presents a critical gap in the country's fight against OCSEA. Without being a signatory, Tanzania is excluded from direct access to international cooperation mechanisms, such as the 24/7 cybercrime contact points, expedited data preservation, and procedural cooperation that the Convention mandates. The absence of this treaty in Tanzania's legal framework significantly hinders cross-border investigations, particularly in cases involving international online grooming networks, darknet CSAM exchanges, or perpetrators using offshore servers. Moreover, as OCSEA cases often involve perpetrators operating from different jurisdictions, the lack of ratification complicates evidence gathering, delays mutual legal assistance, and weakens the capacity to pursue justice effectively.

Nevertheless, Tanzania has incorporated some Budapest principles domestically through laws such as the Cybercrimes Act, Cap 443, and Electronic and Postal Communications (Online Content) Regulations, GN No. 538, particularly regarding unauthorized access, system interference, and basic content regulation. However, these remain fragmented and insufficient, especially in the absence of legally binding international cooperation frameworks. By ratifying the Budapest Convention, Tanzania would not only align itself with international best practices

²³ Council of Europe, Convention on Cybercrime (Budapest Convention) (adopted 23 November 2001, entered into force 1 July 2004) ETS No. 185 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> accessed 16 September 2025.

²⁴ Budapest Convention, Article 9, 2, 4, 5

²⁵ Ibid, Article 10

but also gain access to vital global cybercrime enforcement networks, improve legal and institutional responses to OCSEA, and enhance capacity-building opportunities through collaboration with experienced cybercrime units globally.

2.1.5 Comparative Analysis

Collectively, these four instruments demonstrate complementary but incomplete approaches to combating OCSEA. The UNCRC and the African Charter provide strong human rights foundations emphasizing children's protection, dignity, and best interests. However, both instruments were drafted before digital technologies transformed patterns of child sexual exploitation and therefore, require dynamic interpretation and legislative supplementation.

By contrast, the Budapest Convention and the Malabo Convention focus primarily on cybercrime regulation and digital investigations rather than child protection itself. While they provide valuable procedural tools for investigating online offences, they do not offer comprehensive child rights frameworks comparable to the UNCRC or ACRWC.

A persistent challenge across all four instruments is implementation. Legal obligations frequently exceed States' institutional capacity, particularly in developing countries where shortages of technical expertise, financial resources, digital infrastructure, and international cooperation mechanisms hinder effective enforcement. In addition, the transnational nature of OCSEA creates jurisdictional conflicts, delays in mutual legal assistance, inconsistent criminal definitions, and evidentiary challenges.

Another common policy issue concerns balancing cybersecurity, criminal justice, privacy, freedom of expression, and children's rights. Expanding governmental powers to detect and investigate online exploitation must be accompanied by independent oversight, judicial authorization, proportionality, and respect for international human rights standards.

2.2 The Legal and Institutional Framework for Protecting Children From Online Sexual Exploitation and Abuse In Tanzania

2.2.1 The Constitution of the United Republic of Tanzania, Cap 2

The Constitution of the United Republic of Tanzania, 1977 Cap 2, serves as the supreme law of the land and lays the foundational principles for the protection of human rights and the administration of justice in Tanzania. While the Constitution does not directly mention Online Child Sexual Exploitation and Abuse (OCSEA), it sets out essential rights and protections that indirectly establish a constitutional basis for safeguarding children from online harms.

Article 11 of the Constitution recognizes the special position of children in Tanzanian society.²⁶ It obligates the state and all public institutions to ensure that children are protected against all forms of harm, including abuse, neglect, and exploitation. Though the provision uses general terms, its broad scope justifies legislative measures aimed at combating emerging threats such as OCSEA. The Constitution thus provides a legitimate basis for the state to regulate internet use and digital spaces to protect minors from sexual exploitation and abuse.

Further, Article 12(1) provides that every person is entitled to recognition and respect for their dignity. This provision underscores the importance of protecting the personal integrity of children who may be subject to online sexual abuse, including grooming, sextortion, and the dissemination of exploitative images. OCSEA clearly violates a child's dignity, and hence, preventive legal frameworks are constitutionally warranted.²⁷ Article 13(6)(a) guarantees every person's right to a fair hearing before any action is taken against them. This constitutional guarantee is also significant in the context of online child abuse, particularly during criminal proceedings involving perpetrators and the procedural rights of victims. The principle ensures that both victims and accused persons are treated fairly in judicial processes, and it calls for the development of procedural safeguards, including the protection of child victims during court proceedings.²⁸

Additionally, Article 14 protects the right to life, and Article 16(1) upholds every person's right to privacy and personal security. These provisions are particularly relevant to OCSEA cases, where children's lives and safety are put at risk by the proliferation of child sexual abuse material (CSAM), livestreamed abuse, and online grooming. The right to privacy is especially crucial in the context of data protection, digital surveillance, and the regulation of content on digital platforms.²⁹ Although the Constitution does not specifically reference cybercrimes or OCSEA, its rights-based framework justifies the development and application of specialized statutes, such as the Cybercrimes Act, the Law of the Child Act, and the Electronic and Postal Communications (Online Content) Regulations, which operationalize constitutional principles in the digital context.

Moreover, Tanzania's constitutional commitment aligns with its obligations under international instruments like the United Nations Convention on the Rights of the Child (CRC), to which it is a signatory. Therefore, the Constitution remains a foundational text upon which more focused child protection laws and policies addressing OCSEA are built.³⁰

²⁶ The Constitution of United Republic of Tanzania, 1977, Article 11

²⁷ Ibid, Article 12 (1).

²⁸ Ibid, Article 13 (6)(a).

²⁹ Ibid, Article 14, 16 (1).

³⁰ United Nations Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC).

2.2.2 The Law of the Child Act, Cap 13

The Law of the Child Act, Chapter 13, Revised Edition 2019, serves as the principal legal instrument safeguarding children's rights and welfare in Tanzania. Enacted to domesticate the United Nations Convention on the Rights of the Child (UNCRC) and the African Charter on the Rights and Welfare of the Child (ACRWC), the Act embodies a comprehensive legal framework focused on promoting the best interests of the child across various dimensions, including care, protection, parental responsibility, and protection from abuse.

One of the key elements of the Act is its recognition of the evolving threats facing children, particularly with the rise of technological and digital platforms, though it still leans heavily towards traditional and offline harms. The Act defines a child under Section 4 as "a person below the age of eighteen years," and under Section 5 guarantees protection against discrimination based on gender, age, or any other status that could render the child vulnerable.³¹ Importantly, Part II of the Act, titled "Rights and Welfare of the Child," establishes a set of fundamental rights, such as the right to be protected from torture, cruel, inhuman, or degrading treatment through Section 13 and the right to opinion and expression under Section 11.³² These provisions serve as a moral and legal foundation for protecting children in all settings, including online environments.

The protection framework continues under Part III of the Act, which defines "child care and protection" and introduces a statutory duty for the state to intervene when a child is in need of protection. Under Section 17, a child is considered in need of care and protection if they are being sexually abused or are at risk of being sexually abused, even though there is no explicit mention of online dimensions to such abuse.³³

Furthermore, Section 26 of the Act establishes rights of the child when parents are separated, including emotional safety, which can be considered relevant in digital contexts such as online manipulation by separated guardians or third parties.³⁴ Despite its broad commitment to child welfare, the Act lacks express and detailed provisions dealing with digital-specific risks such as online grooming, livestreaming abuse, sextortion, and cyberbullying.

Moreover, Section 33 prohibits publishing information or photographs of a child without due process or permission. While this may provide some measure of digital privacy, it falls short of addressing the dynamic, high-risk nature of OCSEA. There are no procedural guidelines, definitions, or penalties tailored to digital environments or forms of OCSEA, making enforcement difficult and misaligned with the evolving technological landscape.³⁵

³¹ The Law of the Child Act, Cap. 13 [R.E. 2019], ss 4, 5.

³² Ibid, ss 5, 11, 13.

³³ Ibid, s 17.

³⁴ Ibid, s 26.

³⁵ Ibid, s 33.

The provisions relating to protection from abuse and exploitation establish the legal basis for State intervention where a child has suffered sexual abuse, neglect, or exploitation. These provisions empower child protection authorities to remove children from harmful environments, investigate allegations of abuse, and initiate protective proceedings before competent courts. In OCSEA cases, these powers may be exercised where a child is subjected to online grooming, coercion into producing child sexual abuse material, or sexual exploitation facilitated through digital platforms. However, these provisions operate as child welfare measures rather than criminal offences. The criminal prosecution of offenders normally depends on separate legislation, such as penal codes, cybercrime laws, or sexual offences legislation.

The Act also imposes statutory duties on parents and guardians to protect children from abuse, neglect, and exploitation. These obligations require parents to exercise appropriate supervision and care, including protecting children from foreseeable risks. In the digital context, responsibilities of parents may extend to supervising online activities of children, educating them about online safety, and reporting suspected exploitation. Nevertheless, most Children's Acts do not expressly define parental responsibilities in relation to internet use, social media, or digital technologies, creating uncertainty regarding the scope of these obligations in cases involving OCSEA.

The Act further establishes duties for public authorities responsible for child protection. Social welfare officers, child protection officers, and other competent authorities are typically authorized to receive complaints, investigate allegations, coordinate protective interventions, and arrange temporary care where necessary. These institutional responsibilities are particularly important where online exploitation requires immediate intervention to safeguard the child from abuse. However, many statutory frameworks do not expressly require specialized training for officials dealing with digital evidence, online grooming, or technology-facilitated exploitation, limiting their effectiveness in responding to online child sexual exploitation and abuse.

Another important aspect concerns reporting mechanisms. Children's legislation often imposes mandatory reporting duties on professionals such as teachers, healthcare providers, social workers, and law enforcement officers who reasonably suspect that a child has been abused. Mandatory reporting can facilitate early identification of online child sexual exploitation and abuse victims, particularly where behavioral changes or disclosures indicate online exploitation. However, many statutes do not specifically require internet service providers, social media companies, electronic communications providers, or online platforms to report detected child sexual abuse material or suspected online grooming to law enforcement authorities. This omission creates a significant gap because technology companies are frequently the first entities capable of detecting online abuse.

The Act also provides mechanisms for the rescue and protection of child victims. Child protection authorities may remove children from situations of immediate danger, place them in temporary protective care, and initiate court proceedings where necessary. These powers remain relevant where online exploitation is linked to trafficking, commercial sexual exploitation, or abuse occurring within the child's home. Nevertheless, rescue provisions often focus on physical protection and may not adequately address continuing online harm arising from the persistent circulation of child sexual abuse material or ongoing digital contact between offenders and victims.

Counselling, rehabilitation, and reintegration constitute another important component of children's legislation. Many Acts require the provision of psychological support, medical treatment, educational assistance, family counselling, and social reintegration services for children who have experienced abuse. These provisions reflect the principles contained in Article 39 of the United Nations Convention on the Rights of the Child, which recognizes children's right to recovery and reintegration. In OCSEA cases, however, rehabilitation frequently requires specialized services addressing trauma associated with the permanent online availability of abuse material, digital victimization, cyberbullying, and fear of repeated dissemination.³⁶ General counselling provisions may therefore be insufficient unless supported by specialized digital victim support programs.

From a criminal law perspective, an important limitation of many Children's Acts is that they do not create specific offences addressing technology-facilitated child sexual exploitation. Conduct such as online grooming, possession or distribution of child sexual abuse material, livestreamed sexual abuse, sextortion, or exploitation through encrypted communications is often regulated by separate cybercrime legislation or sexual offences statutes. Consequently, the Children's Act primarily functions as a protective and welfare framework rather than a comprehensive criminal justice instrument.

Thus, the Children's Act makes an important contribution to combating OCSEA by establishing child protection mechanisms, imposing duties on parents and public authorities, providing reporting obligations, facilitating rescue, and promoting counselling and rehabilitation. However, its primary emphasis remains the welfare and protection of children rather than the criminalization of online sexual exploitation. Effective responses to OCSEA therefore, require the Children's Act to operate alongside cybercrime legislation, sexual offences laws, electronic communications regulations, and data protection legislation. Greater statutory recognition of digital harms, mandatory reporting by technology companies, child-sensitive investigative procedures, and specialized rehabilitation services would significantly strengthen the legal framework for protecting children from online sexual exploitation.

³⁶ The United Nations Convention on the Rights of the Child, Article 39

2.2.3 The Cybercrimes Act, Cap. 443

The Cybercrimes Act, Cap 443 is a central piece of legislation in Tanzania addressing offences committed through or facilitated by the use of computers and digital networks. It was enacted in response to the growing threat of cyber-enabled crimes, including offenses targeting children. The Act criminalizes a range of activities that directly or indirectly pertain to online OCSEA). However, as this section will demonstrate, although the Act marks a progressive move in tackling cyber-related offences, it remains limited in scope and fails to sufficiently address emerging forms of OCSEA such as grooming, livestreamed abuse, and sextortion.³⁷

Section 13 of the Cybercrimes Act specifically criminalizes the production, distribution, possession, or access of child abuse material.³⁸ The offence extends beyond the production of child sexual abuse material to include its publication, procurement, importation, exportation, making available, transmission, and other forms of electronic dissemination. The provision therefore enables prosecution of individuals who create, share, download, or store child sexual abuse material using digital technologies. This section provides Tanzania with a clear substantive criminal offence capable of addressing one of the most prevalent forms of OCSEA. By criminalizing both production and possession, the provision recognizes that demand for child sexual abuse material contributes directly to the continued abuse of children. It also facilitates investigations involving computers, mobile devices, cloud storage, and online communication platforms.

The provision primarily targets abuse material and does not expressly criminalize online grooming, sexual solicitation of children through electronic communications, sextortion, or livestreamed child sexual abuse. Consequently, prosecutors may need to rely upon provisions contained in other legislation, including the Sexual Offences Special Provisions Act, Cap 101, the Penal Code, Cap 16 or the Law of the Child Act, Cap 13 to address conduct occurring before abuse material is produced.

In addition, Section 14 addresses the issue of sending offensive content through communication systems, which could be interpreted to apply to sextortion or unsolicited explicit materials sent to children. However, the provision is broadly framed and lacks specificity regarding child victims.³⁹ Moreover, Section 13 criminalizes unlawful access to computer systems, a clause that could apply to hackers accessing devices or accounts of children to extract or manipulate sexual content.⁴⁰ The Act further criminalizes cyberbullying under Section 23⁴¹ and cyberstalking under Section 24⁴², both of which may overlap with forms of online grooming or coercion that children

³⁷ The Cybercrimes Act, 2015 Cap. 443, R.E 2022

³⁸ The Cyber Crime Act, 2015 Cap. 443, s13

³⁹ Ibid, s 14

⁴⁰ Ibid, s 13

⁴¹ Ibid, s 23

⁴² Ibid, s 24

experience. However, these sections are not child-specific, and the Act lacks a dedicated section on grooming or luring children online.

Section 30 of the Act establishes the jurisdiction of Tanzanian courts over cybercrime offences committed within or affecting Tanzania. This provision is particularly relevant to OCSEA because online sexual exploitation frequently involves offenders, victims, internet servers, and digital platforms located in different countries. The jurisdictional framework enables Tanzania to investigate offences having a sufficient territorial or legal connection with the country.

Nevertheless, jurisdiction alone cannot overcome the practical challenges associated with transnational cybercrime. Effective prosecution often depends upon mutual legal assistance, extradition, and timely cooperation with foreign law enforcement agencies. Where evidence is stored on servers located outside Tanzania, investigators may encounter significant procedural delays and jurisdictional barriers.

Section 39 provides that service providers are generally under no obligation to monitor information transmitted or stored through their systems. This provision reflects the principle that internet intermediaries should not be subject to a general duty of surveillance over users' communications.

While this approach protects innovation and limits excessive monitoring obligations, it presents challenges for combating OCSEA. Internet service providers (ISPs), hosting companies, and social media platforms are frequently the first entities capable of detecting child sexual abuse material or identifying suspicious online behavior. Because the Act does not impose mandatory reporting obligations relating to detected child sexual abuse material, opportunities for early intervention may be lost. In contrast, several other jurisdictions require electronic service providers to report identified CSAM to designated authorities.

Also Part IV of the Act provides extensive investigative powers relevant to cybercrime investigations. Section 31 authorizes search and seizure of computer systems and electronic devices. Sections 32 to 35 permit disclosure of stored computer data, expedited preservation of electronic evidence, and collection of traffic and content data. Sections 36 to 38 regulate court orders, forensic examination, and judicial procedures relating to electronic evidence. These provisions are fundamental to investigating OCSEA because digital evidence is often highly volatile and can be deleted or altered quickly.

In OCSEA investigations, these powers enable law enforcement agencies to preserve communications between offenders and children, recover deleted files, identify internet protocol addresses, trace digital financial transactions, and obtain electronic records necessary to identify offenders and rescue victims. The expedited preservation provisions are particularly important because OCSAM may be removed or transferred across jurisdictions within a short period.

While the Act makes significant strides in criminalizing digital offences, it suffers from conceptual and practical gaps in protecting children from evolving forms of online abuse: Lack of Grooming Provisions: The Act does not explicitly criminalize online grooming, the process where offenders build trust with children online to facilitate abuse. This omission is problematic given the prevalence of grooming on platforms such as Facebook, Instagram, and WhatsApp, where perpetrators often begin with innocent conversations before escalating to explicit content or coercion.

No Coverage for Livestreamed Abuse: The Act is silent on live broadcasting of child sexual exploitation, an emerging form of abuse where perpetrators pay for children to perform sexual acts in real-time via webcams. This legal silence makes it difficult to prosecute such cases, especially where the abuse is facilitated across borders.

Sextortion Not Recognized: Sextortion, where offenders threaten to release sexual images of a child unless further images or sexual favors are provided, is not defined or criminalized under the Act. This leaves a significant gap, especially since evidence from the Disrupting Harm in Tanzania study indicates that sextortion is a growing form of OCSEA in the country. Insufficient Provisions on Digital Evidence: Although cybercrimes inherently involve digital footprints, the Act does not provide robust procedural guidelines on preserving, authenticating, or presenting digital evidence in court. This undermines the successful prosecution of OCSEA cases, which often hinge on complex digital trails.

In practice, enforcement of the Cybercrimes Act is hindered by institutional constraints. Police and prosecutors often lack the necessary training in cyber-forensics and digital evidence management, limiting their ability to investigate or prosecute OCSEA cases effectively. According to a 2022 Disrupting Harm report, only 3% of online sexual exploitation cases in Tanzania resulted in prosecution, mainly due to lack of digital skills, technological infrastructure, and legal clarity.⁴³ Furthermore, Tanzania has not ratified the Budapest Convention on Cybercrime, which could otherwise offer a robust framework for international cooperation, a critical factor since many OCSEA cases involve cross-border elements.⁴⁴

While the Cybercrimes Act, Cap 443 represents an important legal step in addressing internet-facilitated offences, it falls short in addressing the specific and evolving threats posed by OCSEA. The absence of clear provisions on grooming, livestreaming, sextortion, and digital evidence hinders its effectiveness. These legal gaps necessitate urgent reform to align the Act with international best practices and ensure comprehensive protection of children in the digital space.

⁴³ Disrupting Harm in Tanzania (Safe Online, 2022).

⁴⁴ Budapest Convention on Cybercrime, Council of Europe, ETS No.185.

Unlike the Child Act, Cap 13, the Cybercrimes Act, Cap 443 is principally a criminal justice statute rather than a child welfare law. It creates direct criminal offences relating to computer misuse and child pornography while equipping investigators with powers to obtain electronic evidence. Its primary objective is prosecution and enforcement rather than child protection or rehabilitation.

Accordingly, the Act contains no comprehensive provisions concerning the rescue of child victims, emergency protection measures, family interventions, counselling services, or long-term rehabilitation. Once a child victim has been identified, responsibility for protection and welfare shifts largely to other legal frameworks, including the Law of the Child Act, Cap 13, the Sexual Offences Special Provisions Act, and applicable child protection procedures.

Furthermore, the Act imposes duties primarily upon investigators, courts, and individuals subject to lawful investigative orders. It authorizes competent authorities to obtain electronic evidence and requires compliance with court orders concerning disclosure and preservation of computer data. However, it does not impose comprehensive statutory duties upon parents, guardians, schools, or child protection institutions to prevent online exploitation or educate children regarding digital risks. Although service providers may be required to cooperate during investigations, the Act does not establish comprehensive obligations requiring proactive detection of child sexual abuse material, implementation of child online safety measures, or reporting of suspected online grooming.

The absence of these provisions reflects the Act's primary focus on cybercrime enforcement rather than children's rights. Consequently, effective responses to OCSEA require coordinated implementation alongside child protection legislation and multidisciplinary services involving police, prosecutors, social welfare officers, psychologists, healthcare providers, and educational institutions.

.

However, the Act remains primarily an enforcement-oriented statute rather than a comprehensive OCSEA framework. It does not expressly criminalize online grooming, livestreamed child sexual abuse, or sextortion; it lacks mandatory reporting obligations for internet intermediaries; it provides limited regulation of digital platforms; and it contains no child-specific procedures for reporting, rescue, counselling, rehabilitation, or long-term recovery. These deficiencies mean that the Cybercrimes Act cannot operate effectively in isolation. A comprehensive response to OCSEA requires its integration with the Law of the Child Act, Cap 13, the Penal Code, Cap 16, the Sexual Offences Special Provisions Act, Cap 101, the Personal Data Protection Act, Cap 44 and international cooperation mechanisms. Future legislative reform should modernize the Act

by expressly addressing emerging forms of online child sexual exploitation, strengthening platform accountability, and incorporating child-centered procedural safeguards that reflect evolving international standards on children's rights in the digital environment.

2.2.4 The Penal Code, Cap 16

The Penal Code, Chapter 16 is the principal criminal law statute that codifies and penalizes various offenses, including those against children. It plays a foundational role in addressing traditional forms of child sexual abuse, though it lacks specificity in responding to digital or online manifestations of these crimes.⁴⁵ Nevertheless, its relevance to online child sexual exploitation and abuse (OCSEA) remains significant, particularly in defining offences and establishing penal sanctions for acts that could take place either physically or through technological means.

The Penal Code criminalizes various sexual acts against children under its provisions for defilement and indecent assault. Section 130(2)(e) defines rape to include situations where a man has sexual intercourse with a girl under the age of 18 years, with or without her consent, thus removing the element of consent in child sexual abuse cases.⁴⁶ Section 131 prescribes life imprisonment as the minimum sentence when the victim is under the age of ten, illustrating the legislature's intent to offer serious deterrence against sexual abuse of minors.⁴⁷ In addition to rape, Section 135 criminalizes indecent assault against children, defined as any act that is not amounting to rape but involves sexually inappropriate touching or behavior. This covers acts that may not constitute penetrative sex but are exploitative in nature, and can thus encompass several forms of OCSEA such as non-consensual sexual communication or exposure to harmful content.⁴⁸

Although the Penal Code does not explicitly refer to "online" offences or the use of the internet, certain provisions remain relevant in the digital context. For example, Section 138D, inserted through amendments, deals with CSAM by criminalizing the possession, production, and distribution of obscene materials involving children. However, the statute does not define the term "CSAM" clearly, nor does it elaborate on offences such as livestreaming or sextortion, leaving gaps in protection within digital environments.⁴⁹ Moreover, Section 16 of the Cybercrimes Act, Cap 443 rather than the Penal Code, Cap 16 now deals more directly with electronic communications and the transmission of CSAM. The lack of harmony between these laws results in fragmented legal coverage, which may undermine effective prosecution of OCSEA cases.⁵⁰

⁴⁵ Penal Code, Cap. 16 R.E 2029,

⁴⁶ The Penal Code, Cap 16 R.E 2019, s 130(2)(e)

⁴⁷ Ibid, s 131

⁴⁸ Ibid, s 135

⁴⁹ Ibid, s 138D

⁵⁰ The Cybercrimes Act, s16

The Penal Code also criminalizes attempts to commit offences and participation through aiding or abetting, under Sections 380 to 386, which could technically be applied to online grooming or solicitation of children for sexual purposes. However, the lack of explicit definitions or guidance on digital communication as a medium for these crimes limits the practical applicability of these provisions in the context of OCSEA.⁵¹

The Penal Code also criminalizes rape and sexual intercourse with children below the age of consent through the offences of rape and defilement. These provisions are effective where online grooming or digital communication culminates in physical sexual abuse. For example, where an offender uses social media, messaging applications, or online gaming platforms to groom a child before arranging an offline sexual encounter, the completed physical offence falls squarely within the Penal Code.

However, these offences do not adequately address situations in which the abuse remains entirely online. Increasingly, offenders exploit children through live-streamed abuse, coercion to perform sexual acts before a webcam, or manipulation into creating sexually explicit images without any physical meeting. Since the statutory elements of rape and defilement generally require physical sexual penetration or contact, purely virtual sexual exploitation may fall outside their scope. Consequently, the Penal Code leaves a significant gap in protecting children from non-contact online sexual abuse.

The offence of indecent assault may also apply where inappropriate sexual contact occurs following online grooming. It criminalizes indecent acts committed against another person without lawful justification. Nevertheless, its applicability to OCSEA is limited because the offence traditionally contemplates physical touching or contact. Where an offender compels a child to expose themselves during a live video call, send intimate photographs, or engage in sexually explicit conduct through digital platforms, there is no physical assault despite the serious psychological and sexual harm suffered by the child. The absence of statutory recognition of virtual sexual acts creates uncertainty regarding whether courts can interpret indecent assault broadly enough to encompass technology-facilitated abuse.

The Penal Code, Cap 16 contains offences relating to procuration, procurement, and facilitating prostitution or other forms of sexual exploitation. These provisions may apply where offenders recruit or entice children for commercial sexual exploitation using online platforms, social media, or electronic communications. Their usefulness has increased because traffickers and organized criminal groups increasingly rely on digital technologies to identify, recruit, advertise,

⁵¹ The Penal Code ss 380-386

and exploit children. Online advertisements, encrypted messaging applications, and digital payment systems have become common tools in facilitating child sexual exploitation.

However, these provisions were drafted with conventional methods of procurement in mind and do not expressly recognize online recruitment, digital grooming, or technology-enabled coercion. Prosecutors may therefore encounter evidential and interpretive difficulties when attempting to apply traditional procurement offences to modern online conduct.

The Penal Code also criminalizes offences involving obscene publications and distribution of indecent material. At first glance, these provisions appear relevant to CSAM. However, significant legal limitations exist. Traditional obscenity offences were primarily intended to regulate public morality rather than protect children from sexual exploitation. They do not specifically recognize that images depicting child sexual abuse constitute records of criminal victimization rather than merely obscene material.

Furthermore, obscenity offences generally fail to criminalize the full range of conduct associated with CSAM, including possession, intentional access, online distribution, cloud storage, live streaming, or digital transmission across international borders. These shortcomings explain why Tanzania enacted section 13 of the Cybercrimes Act, Cap 443 to specifically criminalize CSAM committed through computer systems⁵².

The Penal Code contains general provisions relating to attempts to commit offences, conspiracy, and aiding or abetting criminal conduct. These provisions may be useful where offenders initiate online grooming with the intention of committing rape, defilement, or trafficking but are intercepted before completing the substantive offence.

For example, an individual who uses online communications to arrange a meeting with a child for sexual purposes may potentially be prosecuted for attempted sexual offences if sufficient evidence demonstrates criminal intent and overt acts towards commission of the offence.

Nevertheless, reliance upon general attempt provisions presents practical difficulties. Online grooming often involves prolonged psychological manipulation rather than immediate preparation for physical abuse. Determining precisely when online conversations become criminal attempts remains uncertain. Consequently, prosecutors may struggle to establish the threshold required for criminal liability before physical contact occurs.

Despite its continuing importance, the Penal Code, Cap 16 exhibits several significant weaknesses in responding to contemporary online child sexual exploitation.

⁵² The Penal Code, Cap 16 R.E 2019, s 13

First, the Code contains no specific offence criminalizing online solicitation or grooming of children for sexual purposes. Law enforcement authorities must therefore wait until more serious conduct occurs before criminal liability becomes clearer, limiting opportunities for early intervention.

Secondly, the Code does not expressly recognize digital coercion or sextortion. Offenders increasingly threaten to distribute intimate images unless children provide additional sexual content or perform sexual acts online. Although elements of extortion or blackmail may apply, the legislation does not specifically address sexually motivated digital coercion involving children.

Thirdly, the Code provides no clear legal recognition of virtual sexual acts. Technological developments such as live-streamed abuse, webcam exploitation, immersive virtual environments, and remote sexual performances challenge traditional concepts of physical sexual offences. The absence of express statutory provisions creates uncertainty regarding criminal liability.

Fourthly, many definitions remain insufficiently child-centered. The Penal Code primarily focuses on prohibited conduct rather than recognizing the unique vulnerabilities of children in digital environments. Contemporary international standards increasingly require legislation that reflects children's evolving capacities, digital privacy rights, psychological harm, and best interests.

Finally, the Penal Code operates largely independently of cyber-investigative procedures. It provides limited guidance regarding electronic evidence, preservation of digital communications, online surveillance, data requests, or cooperation with internet service providers. Successful prosecution of OCSEA therefore depends heavily upon the investigative powers contained in the Cybercrimes Act, Cap 443. Without effective integration between substantive criminal offences and cyber-investigative procedures, enforcement remains fragmented.

The Penal Code, Cap 16 continues to provide an essential legal foundation for prosecuting sexual offences against children in Tanzania. Offences such as rape, defilement, indecent assault, procuration, and attempt remain relevant where online activity facilitates offline abuse. However, these provisions were developed primarily for contact-based criminality and are not well suited to the realities of technology-facilitated child sexual exploitation.

The absence of specific offences addressing online grooming, digital sexual coercion, livestreamed abuse, virtual sexual exploitation, and other non-contact forms of OCSEA creates significant gaps in protection. In addition, the lack of explicit links between the Penal Code and cyber-investigative procedures limits the effectiveness of criminal investigations involving electronic evidence.

To provide comprehensive protection against OCSEA, the Penal Code should be interpreted and applied together with the Cybercrimes Act, Cap 443, the Law of the Child Act, Cap 13, the Anti-Trafficking in Persons Act, Cap 432 and the Personal Data Protection Act, Cap 44. Legislative reform should also introduce specific offences covering online grooming, sexual solicitation of children, sextortion, live-streamed child sexual abuse, and other emerging forms of digital exploitation while strengthening child-centered definitions and integrating substantive offences with modern cyber-investigative procedures.

2.2.5 The Personal Data Protection Act, Cap 44

The Act provides an important legal framework for protecting children's personal data, although it is not the primary criminal law dealing with OCSEA. Its provisions complement criminal laws by safeguarding children's privacy and regulating the handling of their personal information

The Act does not specifically criminalize OCSEA, it supports efforts to combat it by: protecting children's digital privacy, restricting unlawful sharing of children's images and personal information, requiring organizations to secure children's data, providing regulatory oversight through the Personal Data Protection Commission and creating accountability for organizations that mishandle children's personal data.

In Tanzania, criminal offences relating to OCSEA are primarily addressed through other legislation, including the Cyber Crimes Act, Cap 443, Law of the Child Act, Cap 13, and relevant provisions of the Penal Code, Cap 16. The Personal Data Protection Act, Cap 44 complements these laws by ensuring that children's personal data is protected before, during, and after investigations and by regulating how organizations collect, process, store, and disclose such information.

2.2.6 Electronic and Postal Communications (Online Content) Regulations, GN No. 538

The Electronic and Postal Communications (Online Content) Regulations, GN No. 538 represent a critical component of Tanzania's legal architecture concerning digital communications and content management.⁵³ Enacted under the authority of the Electronic and Postal Communications Act, Cap. 306, these Regulations aim to monitor, control, and enforce standards for online content published or disseminated in the country, with implications for the protection of children against online sexual exploitation and abuse (OCSEA).⁵⁴

Regulations 3 explicitly define "prohibited content" to include any material that promotes or depicts child sexual abuse.⁵⁵ Under Regulation 4(1)(j), service providers and content providers are prohibited from publishing, broadcasting, or distributing content that "involves or promotes child pornography." This provision aligns partially with international obligations such as those under the UNCRC Optional Protocol on the Sale of Children, Child Prostitution and Child

⁵³ The Electronic and Postal Communications (Online Content) Regulations, 2020, GN No. 538, 17 July 2020

⁵⁴ The Electronic and Postal Communications Act, Cap. 306.

⁵⁵ The Electronic and Postal Communications (Online Content) Regulations, 2020, GN No. 538, r 3

Pornography, but remains narrowly scoped.⁵⁶ It does not extend to other forms of OCSEA such as grooming, sextortion, or live-streamed abuse.

The Tanzania Communications Regulatory Authority (TCRA) is vested with the mandate to license and penalize online content providers under the Regulations. Providers must adhere to the "Online Content Regulations Code of Conduct," which requires that all content respects the rights of children and does not exploit them in any form. Failure to comply may result in content being taken down, suspension of service, or imposition of fines as provided under Regulations 13 to 16.⁵⁷ However, the absence of robust procedural safeguards and detailed standards for the detection and takedown of OCSEA material limits the practical enforceability of these provisions.

The enforcement framework under the Regulations empowers TCRA to investigate and penalize violations, including the dissemination of child sexual abuse material. Regulation 15 grants the authority to block access to or remove any prohibited content.⁵⁸ In addition, Regulation 17 allows TCRA to impose monetary penalties and suspend licenses for providers who fail to comply.⁵⁹ However, these measures are largely administrative and do not directly facilitate criminal prosecution unless read together with the Cybercrimes Act, Cap 443 or the Penal Code, Cap 16. This gap reflects a lack of harmonization across legal instruments for handling OCSEA cases comprehensively.

While the Regulations signal Tanzania's intent to establish a regulatory environment that considers the safety of children online, they fall short in several key areas. Firstly, the law does not offer a clear definition or comprehensive categorization of OCSEA offences. Secondly, it places the responsibility for content moderation heavily on service providers without a corresponding obligation to report cases to law enforcement or to implement safeguards like age verification, reporting portals, or real-time flagging systems. Lastly, the Regulations do not sufficiently address issues of jurisdiction, data preservation for investigation, or procedures for cooperation with global platforms and law enforcement bodies.

Electronic and Postal Communications (Online Content) Regulations, GN No. 538 play an essential role in restricting access to harmful online material, particularly child pornography. However, their effectiveness in tackling broader forms of OCSEA remains constrained by definitional gaps, weak inter-agency coordination, and limited enforcement mechanisms. These shortcomings underscore the need for Tanzania to enact a dedicated and comprehensive legislative framework for online child protection, ensuring alignment with international best practices and operational capacity.

⁵⁶ Ibid, r 4(1)(j),

⁵⁷ Ibid, r 13-16

⁵⁸ Ibid, r 15

⁵⁹ Ibid, r 17

2.2.7 The Evidence Act, Cap 6

The Evidence Act, Cap 6 plays a pivotal role in facilitating the admissibility and evaluation of evidence in legal proceedings, including those relating to OCSEA. While not a law crafted specifically for the digital era or child protection, it remains a critical procedural statute underpinning the prosecution of cyber-enabled offences. The Act establishes both the framework for what constitutes admissible evidence and the standards required for its authentication and reliability, which are particularly essential when dealing with digital evidence in OCSEA cases.⁶⁰

The prosecution of OCSEA depends primarily upon electronic evidence. Unlike conventional sexual offences, the principal evidence in OCSEA cases frequently consists of electronic communications, digital images, videos, internet protocol (IP) addresses, metadata, cloud records, subscriber information, device extraction reports, and forensic examination of computers and mobile phones. The Tanzania Evidence Act, Cap. 6 therefore plays a central role in determining whether such evidence is admissible, reliable, and legally sufficient to support criminal convictions.

One of the key developments in the Act, introduced via amendments, is the recognition of electronic records and digital evidence as admissible in court. Under Section 2, as amended by the Written Laws (Miscellaneous Amendments) (No. 3) Act, 2018, the definition of “document” now includes electronic records. This provides a legal basis for accepting chat logs, emails, videos, screenshots, and other forms of digital communication that are frequently involved in OCSEA cases.⁶¹

Furthermore, Section 18 of the Act underscores the need for documentary evidence to be both relevant and authentic. This poses challenges for enforcement officers in OCSEA cases, as many of the materials, such as livestream recordings or images shared via end-to-end encrypted applications, require specialized forensic handling to meet evidentiary thresholds.⁶² For instance, Section 66A, which specifically governs the admissibility of electronic records, mandates that they must be produced by a computer in the regular course of its operation and be accompanied by a certificate authenticating its integrity and origin.⁶³

Sections 63 to 66 establish the general rules governing documentary evidence. Section 63 provides that the contents of documents must be proved according to the provisions of the Act.⁶⁴ Section 64 recognizes primary evidence, while section 65 governs the admissibility of secondary evidence. Section 66 identifies circumstances in which secondary evidence may be admitted.

⁶⁰ The Evidence Act, Cap 6 R.E. 2019.

⁶¹ Written Laws (Miscellaneous Amendments) (No. 3) Act, 2018, s 2.

⁶² The Evidence Act, Cap 6, s 18

⁶³ Ibid, s 66A

⁶⁴ Ibid, ss 63-66

These provisions apply to electronic documents because electronic records constitute documentary evidence for evidentiary purposes.

In OCSEA prosecutions, these provisions apply to screenshots of online conversations, emails, social media messages, electronic photographs, downloaded files, and chat histories. Where investigators obtain the original electronic device containing the evidence, the prosecution will ordinarily rely on primary evidence. However, where investigators rely on forensic copies, printed screenshots, exported chat logs, or duplicate electronic records, the court must determine whether the statutory requirements for secondary evidence have been satisfied. The practical difficulty is that electronic records can be duplicated perfectly without altering their content, making the traditional distinction between primary and secondary documentary evidence less straightforward than with paper documents. Consequently, courts focus on authenticity and reliability rather than the physical originality of the document.

Section 64A is the most important evidentiary provision for OCSEA cases because it expressly recognizes the admissibility of electronic evidence.⁶⁵ It enables information generated, stored, copied, or transmitted electronically to be received in evidence, provided that statutory requirements concerning authenticity and reliability are satisfied. This provision significantly strengthens prosecutions involving online child sexual exploitation because the principal evidence often consists entirely of electronic records. Examples include: WhatsApp, Telegram; Signal, and Facebook Messenger conversations; screenshots documenting online grooming; emails arranging meetings with children; child sexual abuse material recovered from computers or mobile devices; cloud storage records; internet browsing histories; metadata establishing the creation, modification, or transmission of files; mobile phone extraction reports; and subscriber information identifying users of online accounts.

Section 64A allows these materials to be considered by the court, thereby overcoming the traditional common law preference for paper documentation. Nevertheless, admissibility under section 64A does not eliminate the prosecution's obligation to establish authenticity.⁶⁶ The court must be satisfied that electronic evidence has not been altered, manipulated, fabricated, or incompletely extracted. This issue has become important because artificial intelligence, image editing software, and encrypted communications create new possibilities for digital manipulation.

Sections 47 to 53 regulate expert evidence.⁶⁷ Section 47 permits the court to receive the opinions of experts on matters requiring specialized knowledge, while sections 48 to 53 regulate the relevance and evidential weight of expert testimony. These provisions are indispensable in

⁶⁵ The Evidence Act, Cap 6, s 64A

⁶⁶ Ibid, s 64A

⁶⁷ The Evidence Act, Cap 6, ss 4,7,5,3

OCSEA prosecutions because judges lack specialized expertise in digital forensic science. Expert witnesses may therefore, testify regarding: forensic extraction of mobile phones and computers; authentication of electronic communications; recovery of deleted files; interpretation of metadata; identification of IP addresses; analysis of internet logs; verification of cloud-based records; detection of digital image manipulation; and preservation of electronic evidence.

Expert evidence enables the court to understand complex technological processes while enhancing confidence in the reliability of electronic evidence. Without such testimony, electronic exhibits may carry reduced evidential weight or be challenged successfully by the defense. However, Tanzania continues to face shortages of qualified digital forensic experts and accredited forensic laboratories. These institutional constraints may delay investigations and affect the quality of expert evidence presented before the courts.

Although section 64A recognizes electronic evidence, admissibility depends upon proper authentication. The prosecution must establish that the electronic record accurately represents the original communication or file and has not been altered after collection. Authentication commonly involves demonstrating: the identity of the device from which the evidence was obtained; the method used to extract electronic data; preservation of metadata; integrity of forensic copies; continuity of possession; and consistency between the electronic record and the original source. For example, where prosecutors rely upon screenshots of online grooming conversations, they should also produce supporting forensic evidence linking those screenshots to the suspect's device or online account. Reliance upon screenshots alone may expose the prosecution to allegations of fabrication or selective editing.

Although the Evidence Act does not contain detailed provisions specifically regulating digital chain of custody, the integrity of electronic evidence remains fundamental to admissibility and evidential weight. In OCSEA investigations, investigators should document: seizure of electronic devices; forensic imaging procedures; transfer of exhibits between investigators; storage conditions; laboratory examination; and production before the court. Maintaining a complete chain of custody reduces the possibility of allegations that electronic evidence was altered, contaminated, or substituted. This is particularly important because electronic files may be copied or modified without obvious physical signs. The absence of detailed statutory procedures governing digital chain of custody means that investigators must rely upon forensic best practices and internal investigative guidelines. Legislative clarification would strengthen the reliability of electronic evidence in cybercrime prosecutions.

Electronic evidence is particularly vulnerable to deletion, remote access, encryption, and automatic destruction through application settings or cloud services. In OCSEA cases, investigators should act promptly to preserve: chat histories; subscriber information; traffic data; cloud records; server logs; deleted files; and metadata. The Evidence Act operates together with

the Cybercrimes Act, Cap 443, whose provisions on preservation orders and disclosure of computer data facilitate the collection and preservation of electronic evidence before trial. Accordingly, admissibility under the Evidence Act depends significantly upon proper preservation procedures undertaken during cybercrime investigations.

A particular hurdle in Tanzania's context is the limited technical expertise and digital forensic capacity to generate or validate such certificates, which hinders the successful prosecution of OCSEA offences. Investigators and prosecutors often lack training and access to tools necessary for preserving digital evidence in line with legal standards. This challenge aligns with concerns raised in previous parts of this chapter, emphasizing that even where laws criminalize OCSEA, the absence of effective evidentiary procedures can obstruct justice.

Moreover, Section 164(1) provides for expert opinion in cases involving technical matters. This can be instrumental in OCSEA cases where digital forensics experts may need to testify about data recovery, encryption, or IP address tracking. However, Tanzania faces a shortage of such qualified experts, especially outside major urban centers, which limits the utility of this provision in practice.⁶⁸

The Evidence Act, Cap 6 provides a sound legal basis for admitting electronic evidence through section 64A and for receiving expert forensic testimony under sections 47 to 53. Together with the documentary evidence provisions in sections 63 to 66, these provisions enable courts to consider the electronic material upon which most OCSEA prosecutions depend.

Nevertheless, the Act remains largely technology-neutral and does not provide comprehensive procedural rules addressing many issues unique to online child sexual exploitation. It contains no detailed provisions governing authentication of cloud-based evidence, block-chain verification, artificial intelligence-generated images, deep-fake technology, encrypted communications, digital chain of custody, or cross-border electronic evidence obtained from foreign technology companies. Nor does it establish child-specific evidentiary protections designed to minimize repeated exposure of victims to child sexual abuse material during criminal proceedings.

Accordingly, although the Evidence Act establishes the legal foundation for admitting electronic evidence, effective prosecution of OCSEA depends upon its coordinated application with the Cybercrimes Act, Cap 443, the Electronic Transactions Act, Cap. 442, the Criminal Procedure Act, the Personal Data Protection Act, 2022, and internationally recognized digital forensic standards. Legislative reform providing detailed procedures for electronic evidence and child-sensitive evidentiary safeguards would further strengthen Tanzania's capacity to prosecute online child sexual exploitation effectively

⁶⁸ Ibid, s 164

2.3 Institutional Framework for OCSEA Enforcement Law Enforcement Agencies (e.g., Cybercrime Unit)

Law enforcement agencies in Tanzania, particularly the Cybercrime Unit under the Tanzania Police Force, play a central role in the enforcement of laws related to OCSEA. The Cybercrime Unit is tasked with investigating technology-facilitated crimes, including offenses involving CSAM, online grooming, sextortion, and other emerging forms of digital child abuse. The Unit operates under the legal framework established by the Cybercrimes Act, Cap 443, which empowers officers to conduct digital surveillance, seize electronic devices, and gather digital evidence relevant to online offenses. However, the enforcement process is often hampered by limited technical capacity, including a shortage of trained digital forensic personnel and inadequate infrastructure to analyze and preserve digital evidence.⁶⁹

2.3.1 The Police Force

The Tanzania Police Force, particularly specialized cybercrime investigators and gender and children protection units, serves as the primary institution responsible for investigating OCSEA offences. Its responsibilities include receiving complaints, identifying victims, preserving electronic evidence, executing search warrants, recovering digital devices, tracing internet communications, identifying suspects, and coordinating with prosecutors.

In OCSEA investigations, police officers may obtain screenshots, chat histories, subscriber information, internet protocol (IP) addresses, metadata, mobile device extraction reports, and digital forensic evidence under the powers provided by the Cybercrimes Act, Cap 443. Prompt action is essential because electronic evidence may be deleted, encrypted, or transferred across jurisdictions within a short period.

However, significant institutional challenges remain. Many police stations lack specialized cybercrime investigators, digital forensic laboratories, and advanced technological equipment. Officers may also have limited training in child-sensitive interviewing techniques, increasing the risk of secondary victimization. Furthermore, cybercrime investigations often require cooperation with foreign technology companies, which can delay access to electronic evidence.

2.3.2 The Office of the Director of Public Prosecutions

The Office of the Director of Public Prosecutions (DPP) plays a central role in evaluating evidence, determining appropriate charges, conducting prosecutions, and coordinating with investigators throughout criminal proceedings. OCSEA prosecutions require prosecutors to understand both substantive criminal law and digital forensic evidence. They must assess whether electronic communications satisfy evidentiary requirements, determine whether offences under the Cybercrimes Act, the Penal Code, or other legislation are applicable, and present complex technical evidence before the courts.

⁶⁹ The Cybercrimes Act 2015, Cap 443.

Despite these responsibilities, specialized prosecutorial expertise in cyber-enabled child sexual exploitation remains limited. Increasing technological sophistication including encrypted communications, cloud storage, cryptocurrency transactions, and artificial intelligence-generated child sexual abuse material requires continuous professional development for prosecutors handling OCSEA cases.

2.3.3 Judiciary (Courts, Case Management, Challenges)

The judiciary in Tanzania is an essential pillar in the enforcement of laws related to Online Child Sexual Exploitation and Abuse (OCSEA). It is responsible for the adjudication of cases involving cyber offenses and ensuring justice for victims. The judiciary ensures that investigations, prosecutions, and trials comply with constitutional guarantees, statutory requirements, and international human rights standards. Judges determine the admissibility of electronic evidence, assess expert testimony, interpret cybercrime legislation, protect children's rights during proceedings, and impose appropriate sentences upon conviction.

Judicial officers also have an important responsibility to minimize secondary victimization. Child victims should receive age appropriate treatment during proceedings through measures such as in-camera hearings where legally permissible, protection of identity, limited exposure to child sexual abuse material during proceedings, and child-sensitive examination procedures.

However, challenges in case management persist, especially in relation to the limited judicial training on technology-facilitated crimes, lack of courtroom procedures for handling digital evidence, and absence of specialized child-friendly courts. Moreover, delays in trials, underreporting, and insufficient collaboration between prosecutors and judicial officers hinder effective resolution of OCSEA cases.⁷⁰ Although a few judges and magistrates have received cybercrime training through ad hoc programs, systemic institutional knowledge remains limited, impacting the judiciary's ability to deliver timely and child-sensitive justice in OCSEA matters.

The rapid evolution of digital technologies also presents interpretive challenges. Courts encounter legal questions concerning electronic evidence, cloud computing, metadata, online anonymity, and cross-border investigations that were not envisaged when many statutes were enacted. Continued judicial training in cybercrime and digital evidence is therefore essential.

2.3.4 Tanzania Communications Regulatory Authorities (TCRA)

The Tanzania Communications Regulatory Authority (TCRA) is established under the Tanzania Communications Regulatory Authority Act, Cap. 172 as the independent regulator of the electronic communications, broadcasting, and postal sectors. Its primary statutory mandate is to regulate communications services, promote fair competition, protect consumer interests, license

⁷⁰ Tanzania Judiciary, Strategic Plan 2020–2025 (Judiciary of Tanzania, 2020).

communications service providers, monitor compliance with communications laws, and facilitate the development of secure and efficient information and communications technologies (ICTs). Although TCRA plays an increasingly important role in responding to cyber-related harms, including Online Child Sexual Exploitation and Abuse (OCSEA), it is not established as a specialized child protection institution or a criminal law enforcement agency. Its contribution to combating OCSEA must therefore be understood within the limits of its statutory mandate.

The statutory framework establishing TCRA does not designate it as a child protection authority comparable to social welfare departments or institutions established under the Law of the Child Act, Cap 13. Unlike child protection agencies, TCRA has no statutory responsibility to: receive reports from child victims; conduct child protection assessments; appoint child advocates remove children from situations of abuse; provide counselling or rehabilitation services; coordinate foster care or family reintegration; or monitor the welfare of child victims. Its role is therefore regulatory rather than welfare oriented. Although TCRA may promote safer internet use through public awareness campaigns and digital literacy programs, these activities complement rather than replace the responsibilities of specialized child protection institutions.

Although TCRA is not a criminal investigative agency, it performs an important supporting role in cybercrime enforcement. The Authority may cooperate with: The Tanzania Police Force; the Office of the Director of Public Prosecutions; cybersecurity institutions; licensed telecommunications operators; and internet service providers. Such cooperation may involve technical assistance, regulatory information, coordination regarding communications infrastructure, or facilitating lawful compliance by regulated communications providers. In OCSEA investigations, this support may assist investigators in identifying subscribers, preserving communications data where authorized by law, tracing network activity, and ensuring compliance by licensed telecommunications operators with lawful investigative requests. However, TCRA cannot independently prosecute offenders, issue criminal warrants, conduct criminal investigations, or determine criminal liability. Those powers remain vested in law enforcement agencies and the courts.

TCRA's principal function is the regulation of electronic communications infrastructure and services. It licenses telecommunications operators, internet service providers (ISPs), broadcasting services, postal operators, and other electronic communications service providers. Through these regulatory powers, TCRA establishes technical and regulatory standards governing the operation of communications networks within Tanzania. TCRA also exercises certain regulatory powers over electronic content made available through licensed communications services. Under subsidiary legislation, including the Electronic and Postal Communications (Online Content) Regulations, it may issue directives concerning unlawful online content, require compliance with licensing conditions, and take administrative action against licensed providers operating within Tanzania.

Although the Authority may issue regulatory directives affecting internet access within Tanzania or engage with local telecommunications operators, it generally lacks jurisdiction to compel foreign technology companies to: remove child sexual abuse material immediately; disclose subscriber information directly; preserve digital evidence; deactivate offending accounts; or modify platform safety features.

In the context of OCSEA, these powers may assist in restricting access to websites or online services that host illegal content or violate Tanzanian communications laws. TCRA may also cooperate with internet service providers to implement lawful blocking measures where authorized by law. Nevertheless, TCRA's role as a content regulator remains limited. The Authority does not operate as a specialized agency responsible for identifying child sexual abuse material (CSAM), conducting criminal investigations, or determining criminal liability. These responsibilities remain with law enforcement agencies and the judiciary. Moreover, content regulation must be exercised consistently with constitutional guarantees relating to freedom of expression, access to information, and procedural fairness. Consequently, TCRA cannot remove online content arbitrarily without legal authority or due process.

This communications regulatory function contributes indirectly to child online protection by ensuring that licensed operators comply with national communications laws, cybersecurity requirements, and lawful directions issued under relevant legislation. TCRA may also require regulated entities to cooperate with lawful investigations conducted under the Cybercrimes Act, Cap 443, or other legislation. However, these regulatory functions do not make TCRA the primary institution responsible for protecting children from online sexual exploitation. Responsibility for child protection remains principally with the Police Force, social welfare authorities, prosecutors, and the courts.

TCRA plays a crucial role in regulating digital content, enforcing compliance with online safety standards, and cooperating with service providers to curb harmful digital practices. Under the Electronic and Postal Communications (Online Content) Regulations, GN No. 538, In relation to OCSEA, TCRA contributes by developing regulatory standards for electronic communications, promoting responsible internet use, supporting cybersecurity initiatives, and facilitating cooperation with licensed communications service providers during lawful investigations. It also undertakes public awareness campaigns promoting safer internet use among children and young people.

TCRA can require removal of illegal content and suspend non-compliant platforms. However, TCRA's enforcement role in child-specific online safety remains limited, with insufficient monitoring of content targeting minors and a lack of proactive collaboration with global platforms such as Facebook, TikTok, or WhatsApp, where most OCSEA incidents occur. The

Authority possesses limited direct powers to compel rapid removal of child sexual abuse material hosted on foreign platforms or to regulate multinational social media companies operating outside Tanzanian jurisdiction. Consequently, its effectiveness often depends upon voluntary cooperation from digital service providers and international regulatory partnerships. Additionally, TCRA lacks specialized child protection units and does not yet impose strict child data protection standards, leaving regulatory gaps in safeguarding children online.⁷¹

2.3.5 Social Welfare and Child Protection Services

Social welfare officers and child protection units, under the Ministry of Community Development, Gender, Women and Special Groups, provide support services to victims of abuse, including psychosocial counseling, temporary shelter, and reintegration. Social welfare officers are central to the protection and rehabilitation of child victims. Unlike criminal justice institutions, whose primary objective is prosecution, social welfare authorities focus on safeguarding children's welfare, conducting risk assessments, arranging temporary care where necessary, providing psychosocial support, coordinating counselling services, and facilitating family reintegration where appropriate.

In OCSEA cases, social welfare officers should participate from the earliest stages of investigation to ensure that children's best interests remain paramount. They also provide essential support during forensic interviews and court proceedings while coordinating long-term rehabilitation services.

However, their response to online abuse remains underdeveloped, as these services were traditionally designed for offline forms of abuse. There is a notable lack of training in handling digital exploitation cases, and coordination between social welfare officers and digital forensic units or police is often weak.⁷² Furthermore, resource limitations, especially at the district and ward levels, restrict their ability to reach children in remote areas who are increasingly exposed to OCSEA risks through mobile technology.

2.3.6 The Personal Data Protection Commission (PDPC)

The Commission plays an important supporting role in preventing and responding OCSEA in Tanzania. While the PDPC is not a criminal law enforcement agency, it regulates how personal data is collected, processed, stored, and shared to protect individuals' privacy, especially that of children. Its roles in relation to OCSEA include: Protecting children's personal data; Monitoring compliance, Receiving and investigating complaints; Promoting public awareness; Supporting law enforcement; Promoting accountability

⁷¹ The Electronic and Postal Communications (Online Content) Regulations, GN No. 133 of 2020 (Tanzania).

⁷² Ministry of Community Development, Gender, Women and Special Groups, Child Protection Guidelines (2021).

The Personal Data Protection Commission contributes to combating OCSEA by protecting children's privacy, ensuring secure processing of personal data, investigating privacy violations, raising public awareness, and supporting lawful handling of evidence. Criminal investigation and prosecution of OCSEA offences remain the responsibility of agencies such as the Police, TCRA, and other competent law enforcement authorities

2.3.7 Schools and Educational Institutions

Schools play an important preventive role within the institutional framework. Teachers are frequently among the first adults to identify behavioral changes indicating possible online exploitation, including anxiety, social withdrawal, unexplained possession of digital devices, fear associated with internet use, or disclosure by students. Educational institutions also contribute by delivering digital literacy programs, promoting online safety education, teaching responsible internet use, and encouraging reporting of online abuse. However, many schools lack formal child online protection policies, specialized teacher training, and established reporting mechanisms for suspected OCSEA cases. Strengthening school based prevention programs would significantly improve early detection and intervention.

2.3.8 Internet Service Providers and Mobile Network Operators

Internet service providers (ISPs) and mobile network operators occupy an increasingly important position because they facilitate electronic communications through which many OCSEA offences occur. These entities may assist criminal investigations by preserving subscriber information, retaining communication records where authorized by law, responding to lawful requests from investigators, and supporting identification of offenders through technical information.

However, Tanzanian legislation imposes only limited proactive obligations upon ISPs regarding detection and reporting of child sexual abuse material. Unlike some jurisdictions that require mandatory reporting of identified child sexual abuse material, the current legal framework relies heavily upon cooperation during investigations rather than active prevention. Balancing investigative cooperation with users' rights to privacy and data protection also presents continuing legal challenges.

2.3.9 Digital Platforms and Technology Companies

Global digital platforms including social media companies, messaging applications, cloud storage providers, online gaming services, and video-sharing platforms have become central actors in preventing and responding to OCSEA. These companies possess sophisticated technologies capable of detecting known child sexual abuse material, identifying suspicious online behavior, removing illegal content, suspending offending accounts, preserving electronic evidence, and cooperating with law enforcement agencies.

In practice, rapid removal of child sexual abuse material is essential because continued online availability results in repeated victimization of children whose abuse continues to circulate indefinitely. Nevertheless, Tanzania's legal framework currently imposes limited statutory duties upon multinational technology companies regarding proactive detection, reporting, or removal of OCSEA-related content. Enforcement is further complicated because many platforms operate outside Tanzanian jurisdiction and are governed by foreign legal systems.

2.3.10 Conclusion

The institutional framework for combating OCSEA in Tanzania demonstrates that protecting children online cannot be achieved through criminal law alone. Effective responses require coordinated action involving law enforcement agencies, prosecutors, courts, regulators, child protection authorities, educational institutions, telecommunications providers, internet intermediaries, and international partners. Each institution performs a distinct but complementary role in prevention, reporting, investigation, evidence preservation, prosecution, victim support, rehabilitation, and public education.

However, the current framework remains characterized by fragmented institutional responsibilities, limited specialist capacity, inadequate coordination, insufficient engagement with digital platforms, and resource constraints. Strengthening inter-agency cooperation through formal referral mechanisms, specialized multidisciplinary OCSEA task forces, joint training programs, clear information-sharing protocols, and stronger partnerships with technology companies would significantly improve Tanzania's capacity to prevent, investigate, prosecute, and respond to Online Child Sexual Exploitation and Abuse while ensuring that child victims receive timely protection, recovery, and reintegration services.

2.4 Methodology

This study employed qualitative legal research approach, grounded primarily in the doctrinal legal method, and supplemented by empirical and comparative legal methods. These methods are appropriate given the study's focus on evaluating the adequacy of Tanzanian law in addressing OCSEA, comparing it with regional and international legal frameworks. The use of doctrinal legal analysis forms the primary method, while empirical methods serve as complementary tools to enrich the depth and applicability of the findings. A total of 22 out of 23 key stakeholders were interviewed, including five law enforcement officers (police/cybercrime unit), three prosecutors, three magistrates, four regulatory or policy officials (TCRA, Ministry, Cybercrime Unit), two child rights advocates or legal aid providers, 4 academicians with expertise in child protection and cyber law, and one citizen representative (such as a parent or community leader with awareness of OCSEA issues).

2.5 Findings

It has been observed that, the laws protect children from online sexual exploitation and abuse via amendments to the Cybercrime Act and Child Act, but it is not yet fully sufficient. There are significant gaps in definitions, policy coherence, enforcement capacity, regulatory oversight of digital platforms, and victim-support. For the framework to be truly adequate, these gaps must be addressed, particularly as digital technologies evolve and new forms of OCSEA emerge. Also, weak monitoring, regulation and enforcement of Child Act lacked a fully established monitoring framework and absence of Cybercrime Regulations undermine online child protection. Therefore, Cybercrime Act and Child Act need to be harmonized in order to have full protection of the children in digital environment.

2.6 Recommendations

The findings of this study demonstrate that Tanzania's legal framework does not adequately address several emerging forms of OCSEA. Legislative reform should therefore move beyond general amendments and introduce precise statutory provisions capable of addressing technology-facilitated child sexual exploitation.

(a) Amend the Cybercrimes Act, Cap 443

The Cybercrimes Act should be amended to include new offences specifically addressing contemporary forms of OCSEA.

First, the Act should introduce a statutory definition of online grooming and create an independent offence criminalizing the intentional use of information and communication technologies to communicate with, befriend, manipulate, recruit, or deceive a child for the purpose of committing sexual exploitation or abuse. The offence should be complete once the offender intentionally engages in grooming behavior with the requisite sexual purpose, without requiring proof that a physical meeting or sexual assault subsequently occurred. This would permit earlier intervention by law enforcement agencies and strengthen the preventive protection of children.

Secondly, the Act should expressly criminalize sextortion involving children. The offence should prohibit obtaining, attempting to obtain, or coercing a child to produce or transmit sexually explicit material through threats, intimidation, blackmail, deception, or abuse of authority. The offence should also criminalize threats to distribute intimate images unless additional sexual content, money, or sexual acts are provided.

Thirdly, the Act should create a specific offence addressing livestreamed child sexual abuse. Criminal liability should extend to any person who organizes, facilitates, transmits, broadcasts,

purchases access to, knowingly views for exploitative purposes, or profits from the live online transmission of child sexual abuse, irrespective of whether a permanent recording exists.

Fourthly, the Act should criminalize online sexual coercion, including conduct involving deception, manipulation, psychological pressure, or technological means used to compel children to participate in sexual activities, expose themselves during video communications, or create sexually explicit material.

Fifthly, the Act should modernize offences relating to CSAM by replacing the term "child pornography" with "child sexual abuse material" to reflect internationally accepted terminology. The legislation should expressly criminalize the production, distribution, dissemination, transmission, advertising, procurement, sale, importation, exportation, possession, intentional access, and facilitation of CSAM through computer systems or electronic communications.

Finally, the Act should create offences addressing the misuse of artificial intelligence (AI) in child sexual exploitation. It should criminalize the creation, possession, dissemination, sale, or distribution of AI-generated or digitally manipulated child sexual abuse material, including deep fake images and synthetic sexual content depicting children. The legislation should also prohibit the use of AI technologies to facilitate online grooming, identity manipulation, or sexual exploitation of children.

(b) Amend the Law of the Child Act, Cap 19

The Law of the Child Act should be amended to recognize children's rights within digital environments. The Act should include statutory definitions of online child sexual exploitation and abuse, online grooming, child sexual abuse material, and digital exploitation. It should expressly recognize children's right to online safety, digital privacy, protection from technology-facilitated abuse, and recovery from online victimization.

The Act should further establish child sensitive procedures governing investigations involving digital offences. These should include specialized forensic interviewing, multidisciplinary child protection teams, mandatory psychosocial assessment, confidential reporting procedures, age-appropriate participation in criminal proceedings, and long-term rehabilitation and reintegration services for child victims of online exploitation. The legislation should also require government institutions to establish coordinated referral mechanisms linking police investigators, prosecutors, social welfare officers, healthcare providers, educational institutions, and counselling services.

(c) Amend the Penal Code, Cap. 16

The Penal Code should be amended to complement the Cybercrimes Act by recognizing technology-facilitated sexual offending. Specific provisions should criminalize sexual exploitation committed entirely through electronic communications, causing a child to engage in sexual acts through video conferencing or live-streaming technologies, attempting to procure sexual activity through online communications and aiding, facilitating, or conspiring to commit OCSEA using digital technologies. These amendments would eliminate uncertainty regarding the application of traditional sexual offences to non-contact digital abuse.

(d) Amend the Evidence Act, Cap. 6

The Evidence Act should be amended to strengthen procedures governing electronic evidence in OCSEA cases. The amendments should establish detailed statutory provisions concerning authentication of electronic evidence, preservation of metadata, chain of custody for digital evidence, admissibility of cloud-based evidence, treatment of encrypted communications, admissibility of digital forensic reports; and specialized evidentiary protections for child victims.

The legislation should also authorize courts to adopt child-sensitive procedures that minimize repeated exposure of victims to child sexual abuse material during criminal proceedings.

(e) Amend the Tanzania Communications Regulatory Authority Act Cap. 172

The TCRA Act should clarify the Authority's role in protecting children within digital communications networks. Without converting TCRA into a criminal investigative agency, the legislation should empower the Authority to coordinate national online child safety initiatives, issue regulatory standards promoting child online protection, require licensed communications providers to implement child safety measures, facilitate cooperation between communications providers and law enforcement agencies and develop codes of practice addressing online child protection. These amendments would strengthen TCRA's preventive and regulatory functions while preserving its primary mandate as the communications regulator.

(f) Establish Statutory Duties for Digital Platforms and Internet Service Providers

The study found that Tanzania's legal framework imposes only limited obligations upon multinational digital platforms and internet service providers regarding OCSEA. Comprehensive legislative reform should therefore, introduce statutory duties requiring digital service providers to report suspected CSAM to competent law enforcement authorities without undue delay, preserve electronic evidence immediately upon receiving lawful preservation requests, retain relevant subscriber information and traffic data for legally prescribed periods, subject to judicial oversight and data protection safeguards, cooperate promptly with lawful investigations and

court orders, establish accessible reporting mechanisms for child sexual exploitation content, remove confirmed child sexual abuse material expeditiously following lawful notification, implement reasonable child safety measures, including age-appropriate design features and risk mitigation systems, publish transparency reports describing actions taken against OCSEA and designate legal points of contact for cooperation with Tanzanian authorities.

These duties should apply in a manner consistent with constitutional guarantees, the Personal Data Protection Act, Cap 44, and internationally recognized principles of necessity, proportionality, judicial oversight, and protection of freedom of expression.

(g) Strengthen International Cooperation

Given the transnational nature of OCSEA, legislative reform should strengthen mechanisms for international cooperation. The law should establish clear procedures governing: cross-border preservation of electronic evidence; mutual legal assistance in cybercrime investigations; expedited disclosure requests to foreign service providers; joint investigations involving foreign law enforcement agencies; cooperation with international organizations combating online child sexual exploitation; and recognition of electronic evidence lawfully obtained through international cooperation. Strengthening these mechanisms would improve Tanzania's ability to investigate offences involving foreign digital platforms, offshore servers, and transnational criminal networks.

2.7 Conclusion

The legislative reforms proposed in this study should not be implemented independently. Instead, Parliament should undertake a comprehensive review of Tanzania's child protection and cybercrime legislation to ensure consistency across the Cybercrimes Act, the Law of the Child Act, the Penal Code, the Evidence Act, the TCRA Act, the Personal Data Protection Act, and related legislation. Harmonizing these statutes with international child protection standards would provide a coherent legal framework capable of preventing, investigating, prosecuting, and responding effectively to Online Child Sexual Exploitation and Abuse while safeguarding the rights and best interests of children in the digital environment.

LIST OF CASES

Commercial Case No. 10 of 2008 HCT Commercial Division Arusha (Un reported)
Jamii Media Company Limited V. The Attorney General and Inspector General of Police,
Miscellaneous civil case cause no. 9 of 2016 High Court of Tanzania (Main Registry), Dar es
Salaam.
Joseph Mwangi v Republic [2022] KEHC 1499 (KLR) [2022].
Lazarus Mirisho Mafie, M/S Shydolya Tours & Safaris V. Odilo Gasper Kelenga Alias Moiso
Gasper, Commercial Case No.10 Of 2008
Omary Nzobalakila Vs Republic, Criminal Appeal no 56 of 2022, TZHC 14678 [2022].
R. v. Salvius Francis Matembo et al, Economic Crime Case No. 21 of 2014 (DSM)
Trust Bank of Tanzania V. Le-Marsh Enterprises Ltd. and Two Others, Commercial Case No.4
of 2000 (unreported).

LIST OF STATUTES AND POLICIES

The Anti- Trafficking in Person Act, Cap 432;
The Child Development Policy 2008.
The Constitution of the United Republic of Tanzania, Cap, 2;
The Cyber Crime Act, Cap 443;
The Electronic and Postal Communications Act Cap, 306;
The Electronic and Postal Communication (Online Content) Regulations, 2018; and
The Evidence Act, 1967 Cap 6;
The law of Child Act, Cap 13;
The Penal Code, Cap 16;
The Personal Data Protection Act, Cap 44;
The Prevention and Combating of Corruption Act, Cap 329;
The Tanzania Communications Regulatory Authority Cap, 172;

BIBLIOGRAPHY

BOOKS

- Abeid, M., Muganyizi, P., Olsson, P. et al. Community perceptions of rape and child sexual abuse: a qualitative study in rural Tanzania. *BMC Int Health Hum Rights* 14, 23 (2014). <https://doi.org/10.1186/1472-698X-14-23>
- Carr, J. "Online child protection: Combatting child pornography on the Internet." (2013).
- Hennink M, Kaiser BN. Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social science & medicine*. 2022, Pp. 292:114523.
- Karpen U. Comparative law: perspectives of legislation. *Legisprudence*. (2012). pp. 149-189.
- Kimey, E, An Assessment of the Protection of Child Rights in Tanzania: Law and Practice (LLM Thesis, 2021).
- Lagazio M, Sherif N, Cushman M. A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security*. 2014. ISSN 01674048. Pp 1-32.
- Magalla, A. "Prevention and detection of cybercrimes in Tanzania as described by Cyber Crime Act, no. 13 of 2015." (2018).
- Matumaini J. Research on national communication policy in Africa and Tanzania. *African Communication Research*. 2010: pp. 1-36.
- Mhina Abeid, Pamela Muganyizi, Pia Olsson et al, 'Community Perceptions of Rape and Child Sexual Abuse: A Qualitative Study in Rural Tanzania' (2014) 14 *BMC International Health and Human Rights* 23, 27.
- Mlyakado BP, Li JC, Jia CX. Online sexual exploitation of adolescents in Tanzania: Explaining help-seeking intention using the theory of planned behaviour. *Children and Youth Services Review*, 2023; Vol.154: pp. 107129. <https://doi.org/10.1016/j.childyouth.2023.107129>
- Mollel, A. Electronic Transactions and the Law of Evidence in Tanzania. Iringa University College, 2007.
- Mwingira, AA. "Elimination of cybercrimes in Tanzania: Law and practice." PhD diss., The Open University of Tanzania, 2013
- Odudu, Q. "Child Abuse: The Emerging Role of The Internet And Technology." (2024).
- Rajani RR. Child sexual abuse in Tanzania: much noise, little justice. *Sex Health Exch*. 1998;(1):13-4. PMID: 12348691.
- Ruellan, L. "The sexual exploitation of children in the digital age. An overview of a major phenomenon in Southeast Asia." (2023). <https://hdl.handle.net/20.500.14239/26134>. Accessed 29 March 2025.

Yonazi, J. "Child Online Protection in Tanzania: Issues That Matter," 2014. Pp 5-6

REPORTS

Fatma Haruna Songoro, Tanzania Amends Cybercrime Act to Boost Child Online Safety

(Victory Attorneys, 23 December 2024)

<https://victoryattorneys.co.tz/2024/12/23/tanzania-amends-cybercrime-act-to-boost-child-online-safety/> accessed 31 March 2025.

Humanium, 'Children's Rights History' (Humanium) <https://www.humanium.org/en/childrens-rights-history/> accessed [1 April 2025].

Safe Online, 'Disrupting Harm in Tanzania – Evidence on online child sexual exploitation and abuse' (December 2022) https://safeonline.global/wp-content/uploads/2023/12/DH_Tanzania_ONLINE_final_191222.pdf accessed 31 March 2025

Save the Children UK, Save the Children UK | International Children's Charity

<https://www.savethechildren.org.uk/> accessed 4 April 2025.

Tanzania Communications Regulatory Authority (TCRA), Quarterly Communications Statistics Report (March 2024)

Tanzania Communications Regulatory Authority, Quarterly Communications Statistics Report (March 2024).

UNICEF (Press Release, 6 February 2018) <https://www.unicef.org/eap/press-releases/more-175000-children-go-online-first-time-every-day-tapping-great-opportunities> accessed 4 April 2025.

United Nations, 'Child and Youth Safety Online' (United Nations) <https://www.un.org/en/global-issues/child-and-youth-safety-online> accessed 15 July 2024.

Electronic and Postal Communications (Online Content) Regulations (Tanzania, 2020).

Tanzania Police Force, Annual Report (2023).

OTHER SOURCES

African Charter on the Rights and Welfare of the Child (adopted 11 July 1990, entered into force 29 November 1999) OAU Doc CAB/LEG/24.9/49.

African Union Convention on Cyber Security and Personal Data Protection 2014.

Ali, S., Haykal, H.A. & Youssef, E. Child Sexual Abuse and the Internet—A Systematic Review. *Hu Arenas* 6, 404–421 (2023). <https://doi.org/10.1007/s42087-021-00228-9> Bakta, Seraphina Msengi. "A critical analysis of the child justice system in (mainland) Tanzania." (2016).

Gilliard, E., Maziko, A., Rwechungura, G., Aliyu, A. A., & Kayumbe, E. (2024). Protecting Africa's Future: Cybersecurity Strategies for Child Safety, Learning, and Skill Acquisition in Tanzania. arXiv preprint arXiv:2409.13159.

Hradova Y, Zhytnyi O, Tereshchuk S. State and legal policy for the protection of children in the digital environment. In International Conference on Social Science, Psychology

- and Legal Regulation (SPL 2021) 2021 Dec 18 (pp. 220-225). Atlantis Press.
- Hryb HM. INTERNATIONAL LEGAL PROTECTION OF CHILDREN'S RIGHTS ON THE INTERNET. ЮРИДИЧНИЙ ВІСНИК. 2022:222.
- Kalmus V, Batista S, Opermann S, Tercova N, Jaron Bedrosova M. Child vulnerability in the digital world. InChild Vulnerability and Vulnerable Subjectivity: Interdisciplinary and Comparative Perspectives 2024 Jul 30 (pp. 131-152). Cham: Springer Nature Switzerland.
- Katz A, El Asam A. Vulnerable children in a digital world. London: Internet Matters; 2019.
- Lafton, Tove, Halla B. Holmarsdottir, Olaf Kapella, Merike Sisask, and Liudmila Zinoveva. "Children's vulnerability to digital technology within the family: A scoping review." *Societies* 13, no. 1 (2022): 11.
- Mbise A, Kaijage T, Mwangosi P, Ng'ondi N, Ndetabura J, Kitembe Z, Chanila D, Minga R. Tanzanian Child Welfare Policy Since British Colonial Rule. *Child Welfare*. 2021 Jan 1;98(6):53-78.
- Musofiana I, Sudarmaji A, Maerani IA. Aspects of legal protection for children from cybercrime. *Jurnal Pembaharuan Hukum*. 2020 Sep;7(3).
- Novianti, N. (2024). Online Child Sexual Exploitation and Abuse (OCSEA) of Children and Adolescents: A Systematic Literature Review. *Psikologika: Jurnal Pemikiran dan Penelitian Psikologi*, 29(2).
- OECD. Children in the digital environment: Revised typology of risks. Paris: OECD Publishing; 2021. Available from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/01/children-in-the-digital-environment_9d454872/9b8f222e-en.pdf [cited 2025 Aug 23].
- Rebhi T. Challenges and Prospects in Enforcing Legal Protection of Children from Online Sexual Exploitation. *Krytyka Prawa*. 2023:21.
- Safe Online, 'Disrupting Harm in Tanzania – Evidence on online child sexual exploitation and abuse' (December 2022) https://safeonline.global/wp-content/uploads/2023/12/DH_Tanzania_ONLINE_final_191222.pdf accessed 31 March 2025
- Sandvik, M. (2022). Protecting children from online sexual exploitation and abuse in the European Union, while encountering challenges and opportunities posed by modern technological development and privacy legislation.
- Shuster, A., Mason, H., & Erwood, S. (2023, November). Online child sexual exploitation and abuse (OCSEA): An escalating problem that is alarming underreported. Child Helpline International.
- United Nations Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.
- WHO (World Health Organization)-Western Pacific Region. (2022). Ending violence against children during COVID-19 and beyond: Second regional conference to strengthen implementation of the INSPIRE strategies. Meeting Report: East

Asia and the Pacific, Virtual Meeting, 1-5 November 2021.

Wijakusumariasih IP. Legal Protection For Children Against Online Sexual Exploitation and Abuse of Children. Jurnal Magister Hukum Udayana (Udayana Master Law Journal). 2003;8:1-2.

APPENDICES

APPENDIX I; INTERVIEW GUIDE

Adequacy and scope of Tanzanian laws in criminalizing emerging forms of OCSEA.

Respondents: Academicians, Magistrates/Judges, Child Rights Advocates

Interview Guide – Academicians

1. How adequate do you consider Tanzania's existing legal framework (e.g., Cybercrimes Act, Penal Code, Law of the Child Act) in addressing emerging OCSEA forms such as grooming, livestreaming, and sextortion?
2. What legal gaps do you see as most critical in weakening the protection of children from OCSEA?
3. In your opinion, to what extent are Tanzanian laws harmonized with international child protection instruments (e.g., UNCRC, ACRWC)?
4. How do you assess the clarity and consistency of definitions in Tanzanian laws regarding OCSEA?
5. What legislative reforms would you recommend to strengthen Tanzania's legal response?

Interview Guide – Magistrates/Judges

1. Based on your experience, do the existing laws provide clear guidance when handling OCSEA-related cases?
2. What challenges do courts face in interpreting and applying current legal provisions on online exploitation?
3. How effective are evidentiary rules in admitting digital evidence in OCSEA cases?
4. Do you find the statutory definitions (e.g., pornography, grooming) comprehensive enough for judicial interpretation?
5. In your view, what amendments would enhance judicial handling of OCSEA cases?

Interview Guide – Child Rights Advocates

1. From your work with children, how sufficient are Tanzania's current laws in protecting victims of OCSEA?

2. What gaps do you encounter in terms of legal remedies for child victims of online exploitation?
3. How responsive is the legal framework to non-contact digital abuse such as sextortion and cyber grooming?
4. Do you find that current laws place adequate obligations on ISPs and digital platforms to protect children?
5. What legal or policy reforms do you think are urgently needed?

Effectiveness of institutional enforcement mechanisms and judicial responses in prosecuting OCSEA cases and ensuring redress for victims in Tanzania.

Respondents: Law enforcement officers, Prosecutors, Magistrates/Judges, Child Rights Advocates/Legal Aid Providers, Regulators & Policy Officials (TCRA, Cybercrime Unit, Ministry of Gender, etc.), Citizens

Interview Guide – Law Enforcement Officers

1. What challenges do you face in detecting, investigating, and prosecuting OCSEA cases?
2. Do you feel adequately trained and resourced in digital forensics for OCSEA investigations?
3. How effective is inter-agency cooperation (e.g., with ISPs, prosecutors, regulators) in addressing online child abuse cases?
4. What barriers exist in securing admissible digital evidence?
5. What reforms or capacity-building measures would strengthen police enforcement?

Interview Guide – Prosecutors

1. How effective is the current legal framework in enabling prosecution of OCSEA offences?
2. What challenges do you face in proving OCSEA cases, particularly with digital evidence?
3. How often do OCSEA cases fail due to legal or procedural gaps?
4. To what extent is inter-agency coordination effective in prosecuting online child abuse?
5. What institutional reforms or legal changes would make prosecutions more successful?

Interview Guide – Magistrates/Judges

1. How frequently do OCSEA cases come before the courts in Tanzania?

2. What are the main judicial challenges in adjudicating such cases (e.g., evidence, definitions, jurisdiction)?
3. How effective is judicial training on handling OCSEA matters?
4. Do current laws support effective sentencing and victim protection?
5. What judicial reforms could improve child protection in online exploitation cases?

Interview Guide – Child Rights Advocates/Legal Aid Providers

1. From your work with victims, how effective are state institutions in providing protection and legal remedies?
2. Do victims of OCSEA receive adequate support in navigating law enforcement and courts?
3. What challenges do you see in coordination between NGOs, police, and prosecutors?
4. How effective are awareness campaigns or prevention strategies in reducing OCSEA?
5. What institutional reforms do you recommend to improve victim-centered responses?

Interview Guide – Regulators & Policy Officials (TCRA, Cybercrime Unit, Ministry)

1. How effective are existing regulatory measures in preventing and addressing OCSEA?
2. What role do ISPs and digital platforms play in enforcement, and how is compliance monitored?
3. How adequate is inter-agency cooperation in policy implementation against OCSEA?
4. What institutional gaps hinder effective regulation of online child exploitation?
5. What policy reforms would strengthen Tanzania's institutional response?

Interview Guide -Citizens

1. How aware are you of the risks of online child sexual exploitation in your community?
2. Do you think Tanzanian institutions (police, courts, regulators) are effective in protecting children online?
3. What challenges do families face when reporting online child abuse cases?
4. Do you trust the justice system to protect victims of OCSEA?
5. What improvements would you suggest to enhance child online safety?