Global Journal of Arts Humanity and Social Sciences
ISSN: 2583-2034

GSAR PUBLISHERS
GLOBAL SCIENTIFIC AND ACADEMIC RESEARCH

OPEN ACCESS

Global Journal of Arts Humanity and Social Sciences
ISSN: 2583-2034
Abbreviated key title: Glob.J.Arts.Humanit.Soc.Sci
Frequency: Monthly
Published By GSAR Publishers
Journal Homepage Link: https://gsarpublishers.com/journal-gjahss-home/

Volume - 6 | Issue - 11 | November 2026 | Total pages 1260-1269 | DOI: 10.5281/zenodo.24170106

CHILD ONLINE SAFETY IN TANZANIA: LEGAL AND INSTITUTIONAL RESPONSES TO EMERGING SOCIAL MEDIA RISKS

By

SHIRIMA, HAIKA J[1], Dr. FRANCISCO MWINZAMHOLYA[2]

[1]LL.M Student, St. Augustine University of Tanzania

[2]Senior Lecturer, St. Augustine University of Tanzania

Article History
Received: 02- 11- 2026
Accepted: 08- 11- 2026
Published: 12- 11- 2026

Corresponding author
SHIRIMA, HAIKA J

Abstract

Children's use of social media exposes them to risks including cyberbullying, online harassment, sexual exploitation, grooming and privacy violations. This study examines the legal and institutional responses to these risks in Tanzania, focusing on the adequacy of existing laws and the responsibilities of relevant institutions.

The study adopts a doctrinal legal approach based on legislation, judicial decisions, international instruments, scholarly publications and institutional reports. It establishes that Tanzania has a legal foundation for child online protection, but challenges remain in institutional coordination, enforcement of platform obligations, identification of offenders and handling of electronic evidence. It recommends stronger implementation of existing laws, improved institutional cooperation and accessible child-friendly reporting mechanisms.

Keywords: child online safety, social media, children's rights, cybercrime, digital privacy, electronic evidence, Tanzania.

1. INTRODUCTION

The increasing use of social media by children has created opportunities for communication, education, access to information and social participation. However, it has also exposed children to cyberbullying, online harassment, sexual exploitation, grooming, harmful content and violations of personal privacy. These risks raise legal concerns because children's rights to dignity, privacy, expression, participation and protection from abuse must also be safeguarded in digital environments.[1]

Tanzania has developed several legal instruments relevant to child online safety. These include the Constitution of the United Republic of Tanzania, 1977, the Law of the Child Act, the Cybercrimes Act, the Personal Data Protection Act and the Electronic and Postal Communications (Online Content) Regulations. Recent amendments, particularly those made in 2024 and 2025, have further strengthened the legal response to child sexual exploitation material and prohibited online content. Nevertheless, the framework operates through different laws and institutions, raising questions about coordination, enforcement and the adequacy of existing protection.[2]

This article examines the legal and institutional responses to social-media risks affecting children in Tanzania. It adopts a doctrinal legal research approach based on legislation, regulations, judicial decisions, international instruments, scholarly publications and institutional reports. It argues that effective child online safety requires coordinated implementation of existing laws, stronger platform accountability, reliable digital evidence procedures and accessible child-friendly protection mechanisms.

[1]United Nations Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25), paras. 12–24 and 35–39.

[2]The Law of the Child Act, Cap. 13, Revised Edition 2023; Cybercrimes Act, Cap. 443, Revised Edition 2023; Personal Data Protection Act, 2022 (Act No. 11 of 2022); Electronic and Postal Communications (Online Content) Regulations, 2020, as amended in 2022 and 2025.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).

2. CHILDREN AND EMERGING SOCIAL MEDIA RISKS

Children's use of social media must be understood within the broader framework of children's rights. Access to digital technology may facilitate education, communication, information and participation. It may also enable children to express their views and maintain social relationships. Accordingly, child online protection should not be interpreted as a general prohibition against children's participation in digital spaces. The legal question is how to protect children from foreseeable harm while respecting their other legally recognised rights.[3]

The definition of a child is central to determining the scope of legal protection. Under section 4(1) of the Law of the Child Act, a child is a person below the age of eighteen years. This approach is consistent with Article 1 of the UNCRC and Article 2 of the African Charter on the Rights and Welfare of the Child. Consequently, the protective framework must address the interests of children across different age groups, taking account of their evolving capacities and circumstances.

One significant category of online risk is cyberbullying. It may involve threatening messages, repeated insults, intimidation, humiliation, harassment or the publication of material intended to cause emotional distress. Unlike some forms of physical bullying, digital harassment may continue beyond the school environment and may reach a child through several online accounts or communication channels. The consequences may affect a child's dignity, psychological well-being, privacy and participation in education and social life.

A second category concerns online sexual exploitation and abuse. Digital platforms may be used to solicit sexual material from children, distribute images or videos involving children, or establish contact with a child for purposes of sexual exploitation. Grooming may involve communication intended to gain a child's trust, manipulate the child or arrange a meeting for sexual purposes. The criminal-law response must therefore address both the production and distribution of exploitative material and preparatory conduct which may lead to abuse.

The significance of these risks is supported by Tanzania-specific research. The *Disrupting Harm in Tanzania* report documents the use of digital technologies in facilitating online child sexual exploitation and abuse. It places online risks within the context of children's access to communication technologies and identifies the need for coordinated action by law-enforcement agencies, child-protection institutions, service providers and families.[4] The report is relevant to the legal analysis because it demonstrates that online sexual exploitation is a practical child-protection issue rather than a purely hypothetical consequence of technological development.

Privacy and personal-data violations constitute another important category. Social-media participation commonly involves the processing of names, photographs, videos, communications, contact details and other information capable of identifying a child. Where such information is collected, used or disclosed without a lawful basis, the resulting harm may extend beyond the initial privacy violation. The information may facilitate harassment, impersonation, exploitation or unwanted contact. Children's particular vulnerability makes the protection of their personal information an essential component of online safety.

The protection of children's privacy must also be balanced against their rights to freedom of expression, access to information and participation. A system that responds to online risks through excessive surveillance or indiscriminate restrictions may itself interfere with children's rights. Article 16 of the UNCRC protects children against arbitrary or unlawful interference with privacy, while articles 12 and 13 recognise children's rights to express views and receive and impart information. General Comment No. 25 requires these rights to be respected in digital environments and emphasises that protective measures should be consistent with the Convention as a whole.[5]

The Organisation for Economic Co-operation and Development (OECD) provides a useful analytical classification of risks affecting children in digital environments. It identifies content risks, contact risks, conduct risks and consumer risks. Content risks arise from material a child may encounter; contact risks arise from interactions with other persons; conduct risks concern the child's own or another person's behaviour; and consumer risks involve commercial practices and exploitation. Privacy and technological concerns may cut across these categories.[6] This classification demonstrates why child online safety cannot be addressed exclusively through criminalization. It also requires regulation of personal-data processing, platform practices, reporting mechanisms and protective education.

The nature of social-media risks is also affected by technological change. New applications, communication features, artificial intelligence tools and algorithmic systems may alter the way children encounter and interact with online content. A legal framework based entirely on the names or characteristics of specific platforms may become outdated. Legal principles should

[3] The African Charter on the Rights and Welfare of the Child, 1990, arts. 4, 7, 10 and 11; Convention on the Rights of the Child, 1989, arts. 12, 13 and 17.

[4] ECPAT International, INTERPOL, & UNICEF Office of Research–Innocenti. (2022). *Disrupting harm in Tanzania: Evidence on online child sexual exploitation and abuse*. Global Partnership to End Violence against Children, particularly pp. 6, 32–34, 45–47 and 58–59.

[5] The Convention on the Rights of the Child, 1989, arts. 12, 13 and 16; United Nations Committee on the Rights of the Child (2021), *General Comment No. 25*, CRC/C/GC/25, paras. 67–71.

[6] The Organisation for Economic Co-operation and Development. (2021). *Children in the digital environment: Revised typology of risks* (OECD Digital Economy Papers No. 302). OECD Publishing, pp. 3–8.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).

therefore be sufficiently technology-neutral to apply to new forms of communication while maintaining clear limits on criminal liability and regulatory intervention.

3. LEGAL ARCHITECTURE FOR CHILD ONLINE SAFETY IN TANZANIA

3.1. Constitutional Protection

The Constitution of the United Republic of Tanzania, 1977, provides the foundation for protecting children's rights in the digital environment. Article 12 protects human dignity, Article 13 guarantees equality before the law, Article 16 safeguards privacy and Article 18 protects freedom of expression and access to information. Article 30 permits lawful limitations on rights where necessary to protect the rights of others and the public interest.[7]

These provisions protect children against online harassment, unlawful disclosure of personal information and other forms of digital abuse. They also require that protective measures respect children's rights to expression and access to information. The Constitution therefore provides the guiding principles for interpreting and applying legislation governing children's online activities.

3.2. Law of the Child Act

The Law of the Child Act, Cap. 13, is the principal statute governing children's rights and welfare in Mainland Tanzania. Section 4(1) defines a child as a person below eighteen years, while section 4(2) establishes the best interests of the child as a primary consideration. Sections 5, 9 and 11 protect against discrimination, safeguard dignity and recognize children's right to express their views. Sections 13 and 16 provide protection against harmful treatment and circumstances requiring care and protection.[8]

The Act also establishes institutional responsibilities. Section 20 provides for the duties of social welfare officers, while sections 94–96 impose child-protection responsibilities on local government authorities, including receiving and investigating reports concerning violations of children's rights. The 2024 amendments introduced section 96A, providing for children's councils.[9]

Although the Act does not specifically regulate social-media platforms, its broad child-protection principles apply where online conduct threatens a child's dignity, safety or welfare. Its effectiveness therefore depends on its interaction with cybercrime, communications and data-protection laws.

3.3. Cybercrimes Act

The Cybercrimes Act, Cap. 443, provides the criminal-law framework for addressing specified offences committed through computer systems. Section 23 criminalizes cyberbullying, while section 13, as amended by the Child Protection Laws (Miscellaneous Amendments) Act, 2024, addresses child sexual abuse material and child sexual exploitation material, including specified conduct involving online grooming and exploitation.[10]

The Act also provides investigative powers. Sections 31–35 address search and seizure, disclosure of data, preservation of computer data and collection of traffic and content data. These provisions are essential where electronic material must be obtained and preserved for investigation and prosecution.[11]

The framework is important because it criminalises particular forms of online abuse and provides legal mechanisms for investigation. However, successful enforcement depends on the ability to identify offenders, preserve digital material and establish the connection between the electronic evidence and the accused person.

3.4. Personal Data Protection

The Personal Data Protection Act, 2022 (Act No. 11 of 2022), regulates the collection and processing of personal information. It is relevant to children because social-media use involves information such as names, photographs, videos, contact details and location data. Section 30 provides safeguards concerning sensitive personal data, including a requirement for parental or guardian consent where the data subject is a minor in the circumstances covered by the provision.[12]

Sections 6 and 7 establish the Personal Data Protection Commission and set out its functions, including supervision of compliance and handling complaints concerning personal-data protection. The Act therefore provides a legal basis for addressing unlawful collection, processing or disclosure of children's personal information. However, further attention is required to child-specific privacy safeguards in the operation of social-media platforms.

3.5. Electronic and Postal Communications Regulation

The Electronic and Postal Communications Act, Cap. 306, regulates electronic communications and provides an additional legal basis for addressing harmful online communication. Section 118 criminalises specified obscene, indecent, false, menacing or offensive communications transmitted through electronic

[7] The Constitution of the United Republic of Tanzania, 1977, arts. 12, 13, 16, 18 and 30.

[8] The Law of the Child Act, Cap. 13, Revised Edition 2023, ss. 4(1)–(2), 5, 9, 11, 13 and 16.

[9] The Law of the Child Act, Cap. 13, Revised Edition 2023, ss. 20 and 94–96; Child Protection Laws (Miscellaneous Amendments) Act, 2024 (Act No. 10 of 2024), inserting s. 96A into the Law of the Child Act.

[10] The Cybercrimes Act, Cap. 443, Revised Edition 2023, s. 23; Child Protection Laws (Miscellaneous Amendments) Act, 2024 (Act No. 10 of 2024), amending s. 13 of the Cybercrimes Act.

[11] The Cybercrimes Act, Cap. 443, Revised Edition 2023, ss. 31–35.

[12] The Personal Data Protection Act, 2022 (Act No. 11 of 2022), ss. 6, 7 and 30.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).

communications facilities or services with the intention of annoying, abusing, threatening or harassing another person.[13]

The Electronic and Postal Communications (Online Content) Regulations, 2020, provide more specific requirements concerning online content. Regulation 18 addresses children's protection from content harmful to their well-being, while regulation 20 provides for complaint handling. The 2022 amendments extended the regulatory framework to include social media and applications. In addition, the 2025 amendments introduced regulation 15A, requiring social-media platform owners to establish mechanisms for filtering and removing prohibited content.[14]

These provisions demonstrate the development of platform-related responsibility in Tanzania. However, their effectiveness depends on enforcement, accessible complaint procedures and cooperation between TCRA, social welfare institutions, law-enforcement authorities and data-protection regulators.

4. INSTITUTIONAL RESPONSE TO CHILD ONLINE RISKS

4.1. Police and Digital Investigation

The Tanzania Police Force has an important role in preventing, detecting and investigating criminal conduct involving children and digital technologies. Its responsibilities are particularly relevant where an online incident may constitute cyberbullying, the distribution of child sexual abuse or exploitation material, grooming or another criminal offence.

The Cybercrimes Act gives authorized law-enforcement officers powers to search and seize, disclose data, preserve computer data, and collect traffic and content data. These powers provide the legal basis for obtaining and preserving information required in digital investigations. They are particularly important where an offender uses an anonymous account or where evidence may be deleted or altered before the investigation is completed.[15]

The investigation of online child abuse may require the examination of mobile devices, social-media accounts, electronic messages, images, videos, subscriber information and other digital records. Investigators must establish not only that the material exists but also how it was obtained, whether it has been altered and how it can be connected to the suspected offender.

The legal framework therefore requires more than the availability of search and seizure powers. Investigators need sufficient technical expertise to preserve digital material, document the process of collection, maintain chain of custody and obtain information through lawful procedures. Where information is held by an online platform outside Tanzania, domestic investigative powers may also need to be supplemented by appropriate cooperation mechanisms.

4.2. Courts and Electronic Evidence

Courts play a central role in determining whether digital material can properly be relied upon in judicial proceedings. In social-media cases, relevant material may include screenshots, electronic messages, photographs, videos, account records, call information and forensic reports. The central evidentiary question is whether the material is relevant, authentic, reliable and sufficiently connected to the person against whom it is presented.

Section 64A of the Evidence Act, Cap. 6, provides that electronic evidence is admissible in proceedings. It further provides that the admissibility and weight of electronic evidence are to be determined in the manner prescribed under section 18 of the Electronic Transactions Act, 2015. Section 18 requires consideration of the reliability of the manner in which a data message was generated, stored or communicated, the reliability of the manner in which its integrity was maintained, the manner in which its originator was identified and any other relevant factor.[16]

Section 19 of the Electronic Transactions Act addresses attribution of electronic communications, while section 20 concerns production of an original document in electronic form. These provisions are important where a prosecution relies on messages or other material obtained from a social-media account. The mere production of a screenshot does not necessarily establish the identity of the person who created or transmitted the communication.

The decision in *Aman Yohana Mwandemile v Republic* illustrates the significance of these requirements. The High Court considered the admission of a flash disk in a criminal prosecution and identified deficiencies concerning the identification of the exhibit, the contents of the electronic material, authentication and compliance with section 18 of the Electronic Transactions Act. The court found that the prosecution had not established the required evidential foundation and allowed the appeal.[17] Although the case did not concern a child or social-media abuse, its reasoning is relevant to the treatment of electronic material in prosecutions involving online conduct.

Similarly, *Livinus Kidamabi @ Tengwa v Republic* involved electronic evidence, including screenshots of WhatsApp communications and a forensic report. The Court considered the statutory criteria under section 18 of the Electronic Transactions Act in assessing the electronic material relied upon in the

[13] The Electronic and Postal Communications Act, Cap. 306, Revised Edition 2023, s. 118.

[14] The Electronic and Postal Communications (Online Content) Regulations, 2020, regs. 18 and 20; Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022, GN No. 136 of 2022; The Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2025, GN No. 57 of 2025, reg. 15A.

[15] The Cybercrimes Act, Cap. 443, Revised Edition 2023, ss. 31–35.

[16] The Evidence Act, Cap. 6, Revised Edition 2022, s. 64A; Electronic Transactions Act, Cap. 442, Revised Edition 2023, ss. 18–20.

[17] *Aman Yohana Mwandemile v Republic*, Criminal Appeal No. 22 of 2021, [2022] TZHC 9520 (High Court of Tanzania, 17 May 2022).

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).

proceedings. The decision illustrates the importance of proper collection, preservation and evidential presentation of digital records.[18]

These decisions demonstrate that the legal question is not merely whether electronic evidence is admissible in principle. The court must also consider its reliability and evidential weight. In child online safety cases, this requirement is especially important because a failure to establish the authenticity or origin of digital material may undermine the prosecution and prevent the child from obtaining an effective judicial remedy.

Judicial officers therefore need a sound understanding of electronic records, digital forensic processes and the relationship between the Evidence Act and the Electronic Transactions Act. Where a child is called as a witness, the child-protection safeguards introduced through the 2024 amendment to section 115 of the Law of the Child Act are also relevant. The requirement for social welfare officer attendance and the power to prescribe child-sensitive cross-examination procedures provide an additional framework for protecting children during proceedings.

4.3. Social Welfare Institutions

Social welfare officers and local government authorities provide the child-protection dimension of the institutional framework. Their responsibilities are important because online abuse may cause psychological, social or family-related harm requiring intervention beyond criminal investigation.

Section 20 of the Law of the Child Act establishes duties relating to care, supervision, advice and counselling of children and their families. Sections 94–96 provide for local-government responsibilities concerning the safeguarding of children, receiving reports of infringements of children's rights and investigating matters requiring protection. These provisions enable social welfare institutions to respond to children affected by online abuse as part of their general child-protection mandate.[19]

The role of social welfare institutions should not be confined to referring a matter to the police. A child affected by online harassment or exploitation may require immediate protection, counselling, family support and referral to other services. Such intervention should be guided by the best-interests principle and should avoid unnecessary disclosure of the child's personal information.

The children councils introduced under section 96A also provide a potential institutional forum for children's participation in matters concerning their rights and welfare. They may contribute to awareness, identification of protection concerns and the development of child-centred approaches to digital safety, provided their activities are supported by appropriate guidance and resources.

4.4. TCRA and Regulatory Response

The Tanzania Communications Regulatory Authority (TCRA) is responsible for regulatory functions within the communications sector. Its role in child online safety is particularly relevant to the regulation of online content, communications services and service providers.

The Electronic and Postal Communications (Online Content) Regulations, 2020, as amended, provide the regulatory framework for children's protection against harmful online content. Regulation 18 imposes an obligation on specified online content actors to take measures to protect children from content harmful to their well-being. Regulation 20 provides for complaint handling, while the 2025 amendment introduced regulation 15A requiring social-media platform owners to deploy mechanisms for filtering and removing prohibited content.[20]

TCRA's role must be distinguished from the criminal-investigation responsibilities of the Police Force and the data-protection responsibilities of the Personal Data Protection Commission. A single online incident may involve several legal issues. For example, publication of a child's intimate photograph may raise questions of prohibited content, criminal liability, unlawful processing of personal information and the child's need for protection. No single institution necessarily has the full responsibility to resolve every aspect of such an incident.

The Personal Data Protection Commission complements TCRA's role by supervising compliance with the Personal Data Protection Act. Sections 6 and 7 of the Act establish the Commission and its functions, including handling complaints and monitoring compliance by data controllers and processors. Its involvement is necessary where the online harm involves unlawful collection, processing or disclosure of a child's personal information.

Effective regulation therefore depends on the ability of TCRA and the Personal Data Protection Commission to exercise their respective mandates and to refer matters to competent authorities where a complaint also involves suspected criminal conduct or a child requiring immediate protection.

4.5. Legal Assistance and Child-Friendly Remedies

Children's access to legal protection depends on the availability of procedures that they and their parents or guardians can understand and use. The existence of a criminal offence or regulatory complaint mechanism does not by itself guarantee that a child will obtain an effective remedy. Legal procedures must be accessible, sufficiently clear and sensitive to the child's age and circumstances.

[18] *Livinus Kidamabi @ Tengwa v Republic*, Criminal Appeal No. 96 of 2022, [2023] TZHC 20779 (High Court of Tanzania, 23 August 2023).

[19] Law of the Child Act, Cap. 13, Revised Edition 2023, ss. 20 and 94–96; Child Protection Laws (Miscellaneous Amendments) Act, 2024, s. 26, inserting s. 96A.

[20] The Electronic and Postal Communications (Online Content) Regulations, 2020, regs. 18 and 20, as amended by GN No. 136 of 2022; Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2025, GN No. 57 of 2025, reg. 7.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).

Advocates and legal-aid providers may assist children and guardians in identifying the legal nature of an online incident and the appropriate institution to approach. Their role is particularly important where the same incident may engage the Cybercrimes Act, the Law of the Child Act, the Personal Data Protection Act and the Online Content Regulations.

Child-friendly remedies should respect confidentiality and minimize the risk of secondary victimization. A child should not be unnecessarily exposed through public disclosure of sensitive photographs, messages or personal information. Proceedings involving children should also take account of the best-interests principle and the child's right to be heard under section 11 of the Law of the Child Act.

The 2024 amendment to section 115 of the Law of the Child Act is relevant in this respect. It requires the attendance of a social welfare officer where a child is called as a witness and empowers the Chief Justice to make rules on cross-examination procedures in matters involving children. These provisions provide a statutory basis for strengthening child-sensitive judicial procedures.

The National Prosecutions Service also forms part of the institutional response through the prosecution of criminal cases. Effective prosecution of cyber-related offences requires appropriate coordination between investigators and prosecutors, particularly in the handling of electronic evidence and assessment of whether the statutory elements of an offence can be proved.

5. CHALLENGES AFFECTING CHILD ONLINE SAFETY

5.1. Anonymity and Identification of Offenders

Anonymity creates a significant legal and investigative difficulty in cases involving social-media abuse. A person may operate an account through a username or pseudonym which does not reveal their actual identity. The child may therefore be able to identify the account from which a threatening message or harmful image was sent without being able to identify the person responsible.

The Cybercrimes Act provides mechanisms for search, seizure, disclosure and preservation of data. However, establishing the identity of an account operator may require information held by telecommunications providers or online platforms. The usefulness of investigative powers consequently depends on whether relevant information remains available, can lawfully be obtained and can be connected to the conduct under investigation.

The problem is not simply the absence of a criminal offence. It is the difficulty of establishing individual responsibility in circumstances where digital identities may be concealed, shared or manipulated. This challenge requires specialized investigation and effective procedures for obtaining and preserving relevant information.

5.2. Electronic Evidence

Electronic evidence presents both technical and legal challenges. Messages, photographs, videos and social-media records may be deleted, edited, copied or redistributed. A screenshot may demonstrate that a particular image or message appeared on a device, but it may not independently establish who created the material, whether it is complete or whether it has been altered.

Sections 64A of the Evidence Act and 18–20 of the Electronic Transactions Act provide the applicable evidentiary framework. The decisions in *Aman Yohana Mwandemile v Republic* and *Livinus Kidamabi @ Tengwa v Republic* demonstrate the importance of reliability, integrity, originator identification and proper evidential presentation.[21]

The legal analysis therefore identifies a need for consistent digital-evidence procedures. Evidence should be collected through lawful processes, properly documented, preserved in a manner that protects its integrity and presented through witnesses capable of explaining its source and handling. Where necessary, specialized digital forensic expertise should be used to support authentication and attribution.

The admissibility of electronic evidence should also be distinguished from its weight. The fact that electronic evidence is admissible does not mean that it automatically proves the truth of its contents or establishes the identity of the accused. The court must assess the statutory criteria and the prosecution must still prove the relevant elements of the alleged offence beyond reasonable doubt.

5.3. Limited Awareness

The legal framework can provide protection only where children and their caregivers are able to identify available rights and procedures. Limited knowledge of reporting mechanisms may delay the preservation of important evidence or prevent a child from obtaining assistance.

This concern is supported by the broader literature on children's digital rights and online safety. The *Disrupting Harm in Tanzania* report demonstrates the importance of access to information and coordinated response mechanisms in addressing online sexual exploitation and abuse. The OECD's risk classification similarly shows that children may encounter a range of risks which require preventive information and appropriate support.[22]

Legal awareness should therefore extend beyond general advice about safe internet use. Children, parents and educators should understand the legal significance of cyberbullying, grooming, unlawful disclosure of personal information and sexual

[21] The Evidence Act, Cap. 6, Revised Edition 2022, s. 64A; Electronic Transactions Act, Cap. 442, Revised Edition 2023, s. 18(2); *Aman Yohana Mwandemile v Republic*, Criminal Appeal No. 22 of 2021, [2022] TZHC 9520; *Livinus Kidamabi @ Tengwa v Republic*, Criminal Appeal No. 96 of 2022, [2023] TZHC 20779.

[22] ECPAT International, INTERPOL, & UNICEF Office of Research–Innocenti. (2022). *Disrupting harm in Tanzania: Evidence on online child sexual exploitation and abuse*; Organisation for Economic Co-operation and Development. (2021). *Children in the digital environment: Revised typology of risks*, pp. 3–8.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).

exploitation. They should also be informed about the available procedures for reporting harmful conduct and seeking assistance.

5.4. Institutional Fragmentation

The Tanzanian framework distributes child online safety responsibilities across different laws and institutions. The Police Force investigates suspected offences; courts determine criminal and civil proceedings; social welfare officers provide child-protection interventions; TCRA regulates online content and communications services; and the Personal Data Protection Commission supervises personal-data processing.

This distribution of responsibilities is not itself a legal defect. Specialised institutions are necessary because online child protection involves criminal law, privacy, communications regulation and welfare. The difficulty arises where the relationship between their respective functions is unclear or referral procedures are insufficiently developed.

For instance, publication of a child's intimate image may involve a criminal offence under the Cybercrimes Act, prohibited content under the Online Content Regulations, unlawful processing of personal information under the Personal Data Protection Act and a need for protection under the Law of the Child Act. A child or guardian should not be required to understand these separate legal regimes before receiving assistance.

The legal framework would therefore benefit from a clear and coordinated referral system identifying the institution responsible for receiving complaints, preserving evidence, assessing immediate risks, investigating criminal conduct and providing welfare support. Such a system should operate through the existing statutory mandates rather than creating overlapping responsibilities.

5.5. Foreign Platforms

The cross-border nature of social-media services creates additional enforcement difficulties. A platform may operate internationally, while relevant subscriber information, account records or other electronic material may be stored outside Tanzania. This can complicate requests for information and the enforcement of domestic legal obligations.

The Cybercrimes Act provides investigative and jurisdictional mechanisms, but the practical effectiveness of those powers may be limited where evidence is held by a foreign-based service provider. The existence of domestic jurisdiction over a particular offence does not necessarily guarantee immediate access to information held in another State.

This issue requires effective international cooperation and structured engagement with relevant service providers. Requests for information must, however, comply with applicable legal requirements and safeguards for privacy and other rights. The objective should be to facilitate lawful access to evidence necessary for protecting children and investigating criminal conduct.

The Online Content Regulations, particularly the 2025 addition of regulation 15A, impose a filtering and removal obligation on social-media platform owners. However, further attention is required to the practical enforcement of that obligation where a platform is established outside Tanzania or where the information needed to respond to a complaint is held in another jurisdiction.

5.6. Technological Change

Social-media platforms and digital technologies continue to develop. New communication features, algorithmic recommendations, automated content generation and other technological developments may create risks that are not fully addressed by provisions drafted with earlier forms of communication in mind.

The Online Content Regulations have been amended to respond to some of these developments. The 2022 amendments expressly brought social media and applications within the definition of online content service. The 2025 amendments introduced obligations concerning filtering, removal of prohibited content and prevention of access to prohibited content through internet services.[23]

Nevertheless, platform safety involves more than removing particular items of prohibited content. It may also concern how services are designed, how users are recommended to children, how children's personal information is processed and how complaints are handled. These matters require a sufficiently clear regulatory approach that protects children without establishing excessive or indiscriminate restrictions on lawful information and expression.

A technology-neutral framework, supported by periodic review of subsidiary legislation and institutional procedures, would be better positioned to respond to new forms of online harm. The law should also distinguish between conduct that constitutes a criminal offence and content that is subject to regulatory restriction. This distinction is essential to legal certainty and the protection of constitutional rights.

6. TOWARDS AN INTEGRATED CHILD ONLINE SAFETY FRAMEWORK

The doctrinal analysis demonstrates that Tanzania already has a legal foundation for protecting children in digital environments. The principal issue is how the existing provisions can be applied coherently and how institutional responsibilities can be translated into practical protection. Strengthening implementation should therefore precede any assumption that a wholly new statute is necessary.

First, the responsible institutions should establish a coordinated child online safety and referral framework. The framework should clarify the respective functions of the Police Force, TCRA, the

[23]Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022, GN No. 136 of 2022; Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2025, GN No. 57 of 2025.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).

Personal Data Protection Commission, social welfare authorities, the National Prosecutions Service and the courts. It should establish procedures for referring complaints involving criminal conduct, prohibited content, personal-data violations and children requiring immediate protection. The framework should also identify the institution responsible for each stage of the response.

Secondly, digital investigative and forensic capacity should be strengthened. Police investigators and prosecutors dealing with online child abuse require training in the lawful collection, preservation and authentication of electronic material. Standard procedures should address documentation of the source of digital evidence, chain of custody, preservation of metadata, forensic examination and requests for information from service providers. These measures would support compliance with section 64A of the Evidence Act and section 18 of the Electronic Transactions Act.

Thirdly, child-friendly reporting mechanisms should be developed at local and institutional levels. A child should be able to report cyberbullying, grooming, sexual exploitation or other harmful conduct without being required to identify the precise legal provision or institution responsible. Schools, social welfare offices and other appropriate child-protection settings should have clear procedures for receiving complaints and referring them to competent authorities. The procedures should protect confidentiality and avoid unnecessary exposure of the child.

Fourthly, the responsibilities of parents and guardians in relation to children's digital participation should be clarified through appropriate guidance and, where necessary, targeted legal development. The Law of the Child Act already recognises parental duties and responsibilities. However, the application of those duties to digital supervision, privacy and online safety requires practical clarification. Measures should encourage reasonable guidance and protection without treating children as having no independent rights to privacy, expression or participation.

Fifthly, platform responsibility should be strengthened through effective implementation of regulation 18 and regulation 15A of the Online Content Regulations. TCRA should ensure that relevant providers understand the obligations imposed by the regulations and that complaints concerning harmful or prohibited content can be addressed through accessible procedures. Further consideration should be given to child-specific safeguards concerning privacy settings, age-appropriate information, reporting facilities and the handling of children's personal information. Any further duties should be clearly defined and consistent with constitutional rights.

Sixthly, the Personal Data Protection Commission should continue to develop and enforce safeguards relating to children's personal information. The application of section 30 to sensitive personal data involving minors should be accompanied by practical guidance for parents, guardians, data controllers and processors. The guidance should explain the lawful processing of children's information, the protection of photographs and identifying information, and the procedures available where personal data are unlawfully disclosed or misused.

Seventhly, the child-protection mandate of social welfare institutions should expressly incorporate online abuse within their operational procedures. Social welfare officers should be able to assess the child's immediate safety and welfare, arrange counselling where necessary and refer criminal matters to the police. Procedures should also protect the confidentiality of digital material received from children and ensure that the child is informed about available assistance.

Eighthly, schools and educational institutions should promote digital rights and online safety education. Such education should address privacy, safe communication, cyberbullying, grooming, harmful content, the protection of personal information and available reporting mechanisms. Children should also be encouraged to participate in discussions about the measures intended to protect them. The children councils established under section 96A of the Law of the Child Act provide a possible institutional forum for such participation.

Finally, legal reform should be based on identified statutory gaps. Tanzania should periodically review the operation of the Law of the Child Act, the Cybercrimes Act, the Personal Data Protection Act and the Online Content Regulations to determine whether their existing provisions are sufficiently clear and enforceable. If further gaps are established, targeted amendments may be preferable to introducing a new statute that duplicates existing mandates. A separate comprehensive child online safety law should be considered only where the existing framework cannot adequately address the identified deficiencies through clarification, coordination or targeted amendment.

7. CONCLUSION

Children's increased use of social media has extended the exercise of their rights into a digital environment in which they may encounter cyberbullying, online harassment, sexual exploitation, grooming, harmful content and violations of personal privacy. These risks require a legal response capable of protecting children while preserving their rights to expression, information, participation and privacy.

Tanzania has developed an important legal foundation for responding to these risks. The Constitution protects dignity, equality, privacy and expression. The Law of the Child Act establishes the best-interests principle and provides for children's welfare, protection and participation. The Cybercrimes Act criminalises specified forms of online conduct and provides investigative powers. The Personal Data Protection Act regulates the processing of personal information, while the Electronic and Postal Communications Act and the Online Content Regulations establish additional requirements concerning harmful online communication and prohibited content.

The legal framework has also developed through recent amendments. The Child Protection Laws (Miscellaneous Amendments) Act, 2024 strengthened the criminal-law framework concerning child sexual abuse and exploitation material and specified online grooming conduct. The 2022 and 2025

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).

amendments to the Online Content Regulations expanded the relevance of communications regulation to social media and introduced additional obligations for internet service providers and social-media platform owners.

However, the existence of protective laws does not alone guarantee effective protection. The doctrinal analysis identifies continuing concerns regarding the interaction of different statutory regimes, the identification of anonymous offenders, the preservation and authentication of electronic evidence, cross-border access to information, the practical enforcement of platform duties and the coordination of institutions responsible for children's protection.

The article therefore concludes that child online safety should be treated as an integrated legal and institutional responsibility. Criminal law, child-protection legislation, data protection and communications regulation must operate together. Effective protection also requires accessible reporting procedures, child-sensitive judicial processes, competent digital investigation, lawful cooperation with online platforms and meaningful participation of children in decisions concerning their welfare.

Tanzania should consequently prioritize the effective implementation and coordination of existing laws, strengthen digital forensic and institutional capacity, improve child-friendly reporting and referral mechanisms, and develop clearer safeguards for children's personal information and digital participation. Further legislative action should be guided by demonstrated gaps and should avoid unnecessary duplication. The objective should be a digital environment in which children can exercise their rights and benefit from social media while receiving effective protection against online abuse and exploitation.

REFERENCES

Books

1. Livingstone, S. (2009). *Children and the internet: Great expectations, challenging realities*. Polity Press.
2. Mambi, A. J. (2010). *ICT law in Tanzania*. Mkuki na Nyota Publishers.

Journal Articles

1. Ayalew, Y. E., Verdoodt, V., & Lievens, E. (2024). General Comment No. 25 on children's rights in relation to the digital environment: Implications for children's right to privacy and data protection in Africa. *Human Rights Law Review, 24*(3), ngae018. https://doi.org/10.1093/hrlr/ngae018
2. John, U. (2021). Legal issues surrounding the admissibility of electronic evidence in Tanzania. *Digital Evidence and Electronic Signature Law Review, 18*. https://doi.org/10.14296/deeslr.v18i0.5290
3. Joseph, E. C., & Mwakisiki, M. E. (2025). Protection of children's rights to privacy in cyberspace: A bird's-eye view over the Tanzanian legal framework. *African Journal on Privacy & Data Protection, 2*, 98–125. https://doi.org/10.29053/ajpdp.v2i1.0002
4. Lukumay, Z. (2024). Foundation for admissibility of electronic evidence in Tanzania. *The Law School of Tanzania Journal, 1*(1), 148–185. https://lstjournal.lst.ac.tz/index.php/files/article/view/26
5. Makulilo, A. B. (2016). The admissibility of electronic evidence in Tanzania: New rules and case law. *Digital Evidence and Electronic Signature Law Review, 13*. https://doi.org/10.14296/deeslr.v13i0.2302
6. Livingstone, S. (2016). Reframing media effects in terms of children's rights in the digital age. *Journal of Children and Media, 10*(1), 4–12.

Reports and Institutional Publications

1. ECPAT International, INTERPOL, & UNICEF Office of Research–Innocenti. (2022). *Disrupting harm in Tanzania: Evidence on online child sexual exploitation and abuse*. Global Partnership to End Violence against Children.
2. Organisation for Economic Co-operation and Development. (2021). *Children in the digital environment: Revised typology of risks* (OECD Digital Economy Papers No. 302). OECD Publishing.
3. Tanzania Communications Regulatory Authority. (2023). *Child online safety guidelines*. TCRA.
4. United Nations Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25). United Nations.

Legislation and International Instruments

1. African Charter on the Rights and Welfare of the Child, 1990.
2. Constitution of the United Republic of Tanzania, 1977.
3. Convention on the Rights of the Child, 1989.
4. Cybercrimes Act, Cap. 443, Revised Edition 2023.
5. Child Protection Laws (Miscellaneous Amendments) Act, 2024 (Act No. 10 of 2024).
6. Electronic and Postal Communications Act, Cap. 306, Revised Edition 2023.
7. Electronic and Postal Communications (Online Content) Regulations, 2020 (Government Notice No. 538 of 2020).
8. Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2022 (Government Notice No. 136 of 2022).
9. Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2025 (Government Notice No. 57 of 2025).
10. Electronic Transactions Act, Cap. 442, Revised Edition 2023.
11. Evidence Act, Cap. 6, Revised Edition 2022.
12. International Covenant on Civil and Political Rights, 1966.
13. Law of the Child Act, Cap. 13, Revised Edition 2023.
14. Personal Data Protection Act, 2022 (Act No. 11 of 2022).

Cases

1. *Aman Yohana Mwandemile v Republic*, Criminal Appeal

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).

No. 22 of 2021, [2022] TZHC 9520 (High Court of Tanzania, 17 May 2022).

2. *Livinus Kidamabi @ Tengwa v Republic*, Criminal Appeal No. 96 of 2022, [2023] TZHC 20779 (High Court of Tanzania, 23 August 2023).

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0).