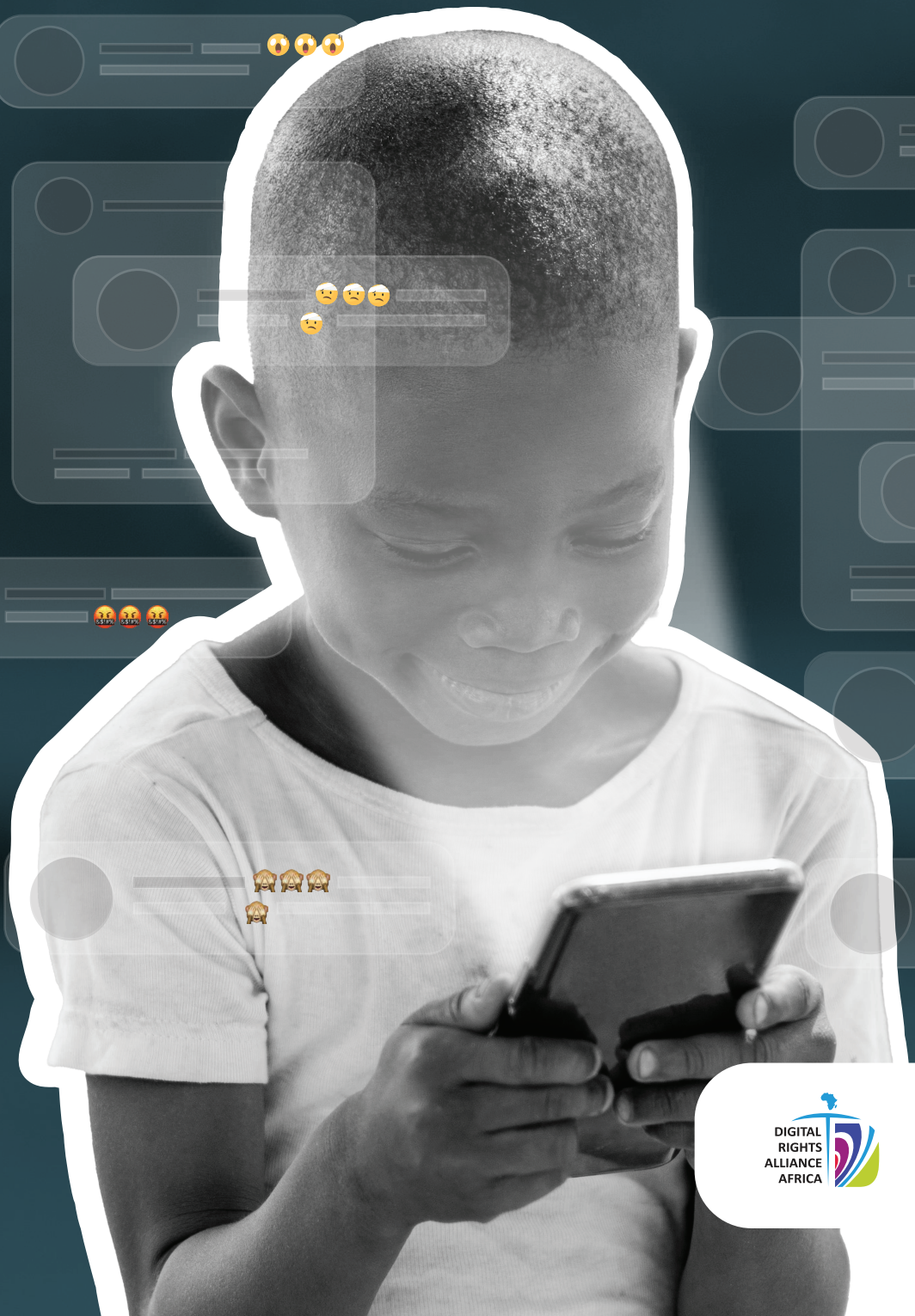
Child Protection and Safety Online in Africa:

The Law, Privacy, Challenges and Solutions

June, 2025



DIGITAL RIGHTS ALLIANCE AFRICA

CIPESA

ICNL

Table of Contents

List of Acronyms

ACRWC	African Charter on the Rights and Welfare of the Child
ASPs	Application Service Providers
AYC	African Youth Charter
CERT	Computer Emergency Response Team
COP	Industry Guidelines for Child Online Protection
CRC	Convention on the Rights of the Child
CSAM	Child Sexual Abuse Material
CSPs	Content Service Providers
DRAA	Digital Rights Alliance Africa
ECOWAS	Economic Community of West African States
GC	General Comment
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
ISOC	Internet Society of Uganda
ISPs	Internet Service Providers
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
KeNIC	Kenya Network Information Centre
KFCB	Kenya Film Classification Board
MCIT	Ministry of Communications and Information Technology
MNR	Model National Response
NAP	National Plan of Action
NCC	Nigerian Communications Commission
NCOPF	National Child Online Protection Framework
NDPR	Nigeria Data Protection Regulation
NITA-U	National Information Technology Authority, Uganda
NITDA	National Information Technology Development Agency
OCSEA	Online Child Sexual Exploitation and Abuse
POPIA	Protection of Personal Information Act
PTSD	Post-Traumatic Stress Disorder
SADC	Southern African Development Community
SAHRC	South African Human Rights Commission
SDGs	Sustainable Development Goals
TCRA	Tanzania Communications Regulatory Authority
UCC	Uganda Communications Commission
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNICEF	United Nations Children's Fund
UNODC	United Nations Office on Drugs and Crime
WSIS	World Summit on the Information Society's

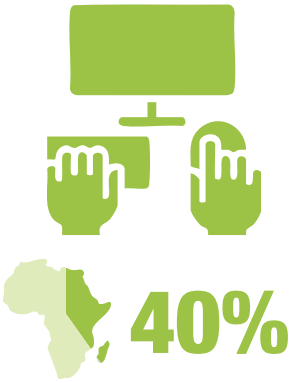
Introduction

The digital landscape in Africa has experienced a transformative shift, reshaping how children engage, learn, and exercise their rights both online and offline.[1] While the challenges of the digital divide remain, an estimated 40% of African children aged 15 and above now have internet access, opening up new avenues for education and connectivity.[2] This trend was accelerated by the COVID-19 pandemic digital revolution, which underscored the importance of digital platforms for learning, social interaction, and access to essential services as in-person activities.

The rapid expansion of digital access for Africa's children and youth has created a complex ecosystem of opportunities and risks, particularly for children. As children increasingly engage in the digital world, the need for specialised protections to address their unique vulnerabilities has become evident, with the right to privacy standing out as both a critical concern and an enabling right. Privacy protections are essential for safeguarding children's safety and supporting their freedom of expression and access to age-appropriate information. Without robust safeguards, children are exposed to risks such as harmful content, data breaches and misuse of their data, and the potential erosion of other fundamental rights.

Recognised as a fundamental human right, children's right to privacy is enshrined in various international, regional, and national legal frameworks. However, in the digital era, ensuring this right is upheld is more urgent than ever due to the attendant risks posed to children.

The report has been produced by the Digital Rights Alliance Africa (DRAA), a network of civil society organisations championing digital civic space, to provide an evidence-based analysis of the key online privacy issues affecting African children, and to advance rights-based protections in the rapidly evolving digital landscape. The report covers 10 African countries, including Algeria, Botswana, Egypt, Ghana, Kenya, Nigeria, Rwanda, South Africa, Tanzania, and Uganda. The findings and recommendations serve as a foundation for advocacy, policy reform, and multi-stakeholder collaborations, aiming to create a safer and more empowering digital environment for Africa's children.



40%

of African children aged 15 and above now have internet access

1 *Article 2 of the African Charter on the Rights and Welfare of the Child defines a child as every human being below the age of 18 years, https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf. Article 1 of the United Nations Convention on the Rights of the Child also provides the same definition.*

2 *The African Union: Child Online Safety and Empowerment Policy (2024), https://au.int/sites/default/files/documents/43798-doc-African_Union_Child_Online_Safety_and_Empowerment_Policy_Feb_2024.pdf .*

The Changing Space of Child Privacy

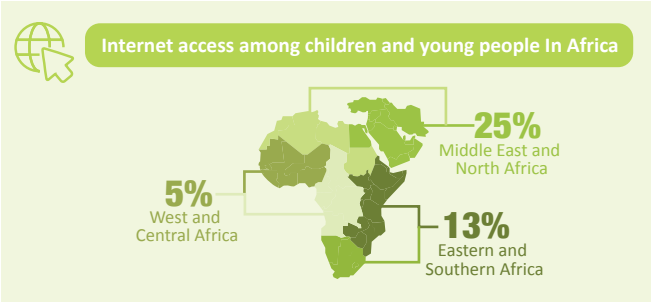
The right to privacy for children is critical for facilitating the enjoyment of civic freedoms online. Over the years, legal standards have been developed to elaborate children's right to privacy in the digital era.

In September 2024, The United Nations Children's Fund (UNICEF) made a call for action for states to protect and prioritise children's rights and safety in digital environments.[3] The call of action recognised the digital era's significant impact on children's livelihood and existing rights.[4] Given the growth of technology and its impact on children, UNICEF called upon key stakeholders to develop and adopt legal and policy reforms to align with the emerging risks to children in the digital era.

Beyond UNICEF, others such as *5Rights Foundation*, *Digital Child Rights Foundation*, and the *Digital Rights Child* in their advocacy for the rights of children, have recognised the emerging risks that children face in the digital era, including, but not limited to, online safety and the violation of their rights to privacy. In this context, reports, statistics and recommendations have been developed as the best way forward to ensure the protection of the right to privacy for children as they enjoy the benefits and insights resulting from accessing digital technologies.[5] The key recommendations according to UNICEF include: the critical nature of Universal connectivity for an inclusive digital future, where all people can participate; explicit prioritization and protection of children's rights and safety in digital environments;

Ensuring that all children and youth have the agency and resources to meaningfully participate in a digital future; and putting in place mechanisms for accountability criteria for discrimination and misleading content.[6] Additionally, internet fragmentation needs to be avoided to ensure an open, free, inclusive, and secure digital future; digital commons, including technologies and services (both existing and emerging), must be accessible, equitable and safe for all children and youth; and, introduce a commons-approach to data governance to protect sovereignty and productive capacity by realizing data as a shared resource for inclusive benefits also for children.[7]

According to a joint UNICEF and International Telecommunication Union (ITU) report, internet access is limited and varies significantly across regions, with only 13% of children and young people in Eastern and Southern Africa having home internet access, 5% in West and Central Africa, and 25% in the Middle East and North Africa.[8] Despite these low figures, research by the Centre for Human Rights on children's online privacy rights in Africa indicates widespread evidence of growing access and governmental initiatives to expand digital access across countries.[9]



3 *UNICEF, "A Brighter Digital Tomorrow: An equitable digital future built for, with and by today's children and young people," https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-submission_UNICEF.pdf*

4 *UNICEF, "Protecting and Prioritizing Children's Rights and Safety in Digital Environments: A Call to Action," https://www.unicef.org/innovation/stories/protecting-childrens-rights-in-digital-environments*

5 *UNICEF, "A Brighter Digital Tomorrow: An equitable digital future built for, with and by today's children and young people," supra.*

6 *Ibid.*

7 *Ibid.*

8 *United Nations Children's Fund and International Telecommunication Union, "How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic." UNICEF, New York, 2020.*

9 *Centre for Human Rights: Pretoria University Law Press (PULP), A study on children's right to privacy in the digital sphere in the African region (2022) at 20, https://www.chr.up.ac.za/images/researchunits/cru/files/publications/Childrens_rights_reports_2022_for_web.pdf*

This simultaneous expansion of access and the persistent digital divide in parts of Africa as noted in the UNICEF and ITU report,[10] and by various scholars and human rights experts, creates a complex challenge for child protection. Moreover, while many children remain excluded from digital opportunities, those gaining access often do so without adequate privacy safeguards or protections against online harms such as cyberbullying, exploitation, and exposure to inappropriate content.

As highlighted by the African Committee of Experts on the Rights and Welfare of the Child, there is a rising concern over online sexual exploitation and radicalisation that requires stronger national and regional responses.[11] This report notes that despite efforts to put in place regional instruments on data privacy, the need to harmonise these frameworks to reflect the complexities of children's privacy rights online within the African context has not been extensively explored. This therefore forms part of a broader call for the urgent need for coordinated legal frameworks within the region that can effectively protect children's privacy and safety without hampering access to digital tools and the internet across the continent.[12]

Accordingly, this research seeks to address the critical gap between increasing access and protection mechanisms for children in Africa. The research pursues this objective by examining the legal and regulatory frameworks for child privacy in online spaces across Africa against international instruments to inform targeted advocacy by civil society actors and other key stakeholders.

10 United Nations Information Service, "Connectivity for everyone is key to Africa's growth and prosperity," https://www.un.org/en/unis-nairobi/connectivity-everyone-key-africa%E2%80%99s-growth-and-prosperity#:~:text=ITU's%202024%20estimates%2C%20released%20in,the%20global%20average%20of%2068%25.

11 See; Report of the African Committee Of Experts on the Rights and Welfare of the Child', ACERWC Report to the Exexutive Council December 2021.pdf

12 OM Sibanda 'Towards a more effective and coordinated response by the African Union on children's privacy online in Africa' (2022) 6 African Human Rights Yearbook, http://doi.org/10.29053/2523-1367/2022/v6a7

Protections and Gaps in Children's Right to Privacy

International Framework

The right to privacy is well-established in international law, and is prominently enshrined under article 12 of the Universal Declaration of Human Rights (UDHR)[13] and further protected in article 17 of the International Covenant on Civil and Political Rights (ICCPR), which stipulates that: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[14]

Everyone has the right to the protection of the law against such interference or attacks.

The right to privacy for children has been expanded under the Convention on the Rights of the Child (CRC), which states in article 16 (1) that no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.[15] However, as technology continues to evolve, the unique challenges related to children's privacy in digital contexts also emerge, prompting the adoption of specific frameworks to address these issues.

General Comment No. 25, 2021 (GC 25) issued by the UN Committee on the Rights of the Child sets out two key duties for states to realise children's privacy rights.[16] These include:

(i) To develop comprehensive data protection frameworks that include special provisions for the processing of children's data, recognising the unique vulnerabilities of children online and offline; and

(ii) To provide parents, guardians, and caregivers with appropriate guidance to effectively safeguard children's right to privacy.

In fulfilling these duties, GC 25 emphasises the importance of states considering their local and cultural contexts that shape understandings of privacy rights in the digital world. However, these requirements seem to be in stark contrast with the human rights framework adopted by the African Union.[17] Specifically, there is a lack of explicit recognition of children's privacy rights in key regional instruments including the African Charter on Human and Peoples' Rights, the Convention on Cyber Security and Personal Data Protection (Malabo Convention), and the African Union Child Online Safety and Empowerment Policy.

13 *Universal Declaration of Human Rights, https://www.un.org/en/about-us/universal-declaration-of-human-rights*
14 *International Covenant on Civil and Political Rights, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights*
15 *Convention on the Rights of the Child, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child*
16 *CRC Committee, General Comment No. 25 (2021) on children's rights in relation to the digital environment, 2021 ("GC25"), https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation*
17 *See, Ayalew, Yohannes Eneyew and Verdoodt, Valerie and Lievens, Eva, 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 (June 14, 2024). Human Rights Law Review, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4875445.*

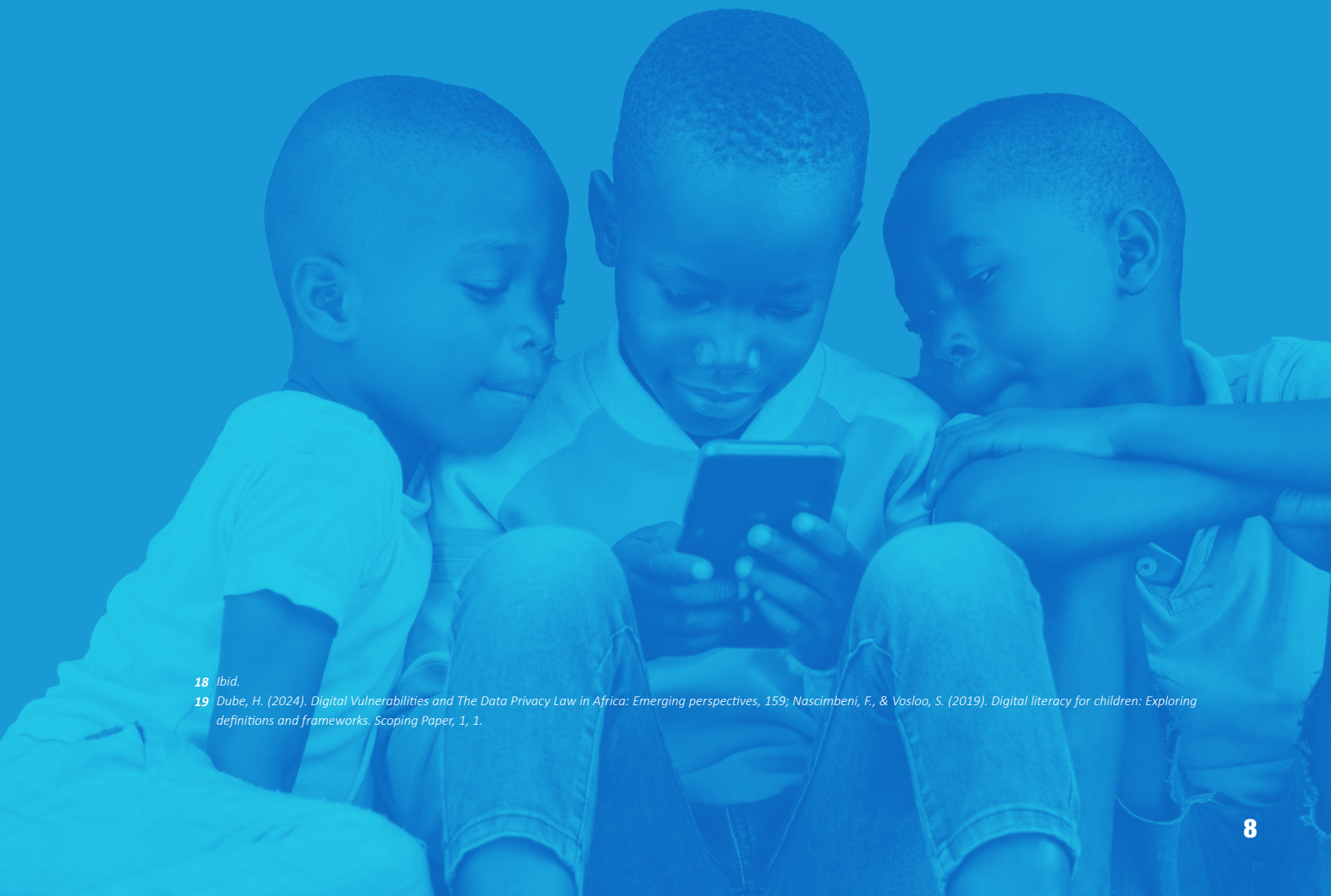
Regarding the second duty stipulated by General comment no. 25, national-level policies and data protection laws in Africa often rely on the consent, capacity and goodwill of parents, guardians or caregivers. This approach assumes that these adults:

1. Fully understand the importance of protecting children's privacy rights and the risks associated with online activity; and

2. Can balance the need for protection with allowing children agency and participation online in line with their evolving capacities.[18]

However, research has shown that parents, guardians and caregivers in Africa frequently lack the critical digital and media literacy skills required to effectively safeguard children's privacy rights while enabling appropriate online access.[19]

While best practices from the European Union's General Data Protection Regulation (GDPR) and efforts to adopt regional instruments in Africa provide important guidance, the concept of harmonising regional frameworks to reflect the complexities of children's privacy rights online within the African context has not been extensively explored.



18 *Ibid.*

19 *Dube, H. (2024). Digital Vulnerabilities and The Data Privacy Law in Africa: Emerging perspectives, 159; Nascimbeni, F., & Vosloo, S. (2019). Digital literacy for children: Exploring definitions and frameworks. Scoping Paper, 1, 1.*

Regional Framework

Africa's regional frameworks provide a different but essential set of protections. While the African Charter on Human and Peoples' Rights[20] does not explicitly address privacy, the African Charter on the Rights and Welfare of the Child (ACRWC)[21] protects children's privacy under article 10: "No child shall be subject to arbitrary or unlawful interference with his privacy, family, home, or correspondence, or to attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children."This provision aims to protect children from arbitrary or unlawful interference with their privacy while balancing this right with parental oversight. This reflects a broader commitment to protecting children's rights under the ACRWC, though state implementation varies significantly.

In 2014, the African Union adopted the Malabo Convention to establish a legal and regulatory framework for cybersecurity and data protection in Africa. The Malabo Convention, which entered into force on June 8, 2023, was highly influenced by the EU data protection framework (the GDPR). It outlines detailed requirements for personal data processing, encourages national data protection authorities to be independent and prioritise personal data protection, and promotes harmonisation of cybersecurity laws across member states. Despite its extensive approach, the Convention faces critical challenges including the absence of the accountability principle in various data protection laws that were enacted prior to the Convention. These laws such as Rwanda, Tanzania, Uganda and Zimbabwe have weak oversight mechanisms that fall short of the obligations set in the Malabo Convention. Additionally, its enforcement is also still low with only *16 ratifications* of the 55 member states.[22] The Malabo Convention also falls short specific provisions on child privacy.[23]

The AU Data Policy Framework provides safeguards for the protection of data relating to children and emphasises the creation of policies to mitigate differential risks that individuals including children face. This calls for specific regulation that is tailored to their needs due to the diverse vulnerabilities they are exposed to and varying levels of digital literacy. Specific mention of data governance for children, including health data and other kinds of sensitive data, is also made.

In 2019, the African Union Commission adopted the *Declaration of Principles on Freedom of Expression and Access to Information.* The Declaration establishes core principles on data processing, including fairness, transparency, and accountability. While the Declaration represents a step forward for data protection across Africa, its focus remains general, with limited provisions addressing children's distinct privacy needs, hence the need for more distinguished normative guidance to strengthen their protection.

The African Union Child Online Safety and Empowerment Policy adopted in 2024 puts in place various principles including on children's right to safety, privacy and participation online.[24] The best interests of the child and non-discrimination are also emphasized. It also sets objectives including institutional capacity development, legal frameworks, and public awareness. It is a guide to support member states in developing strategies and programmes that promote child online safety and empowerment.

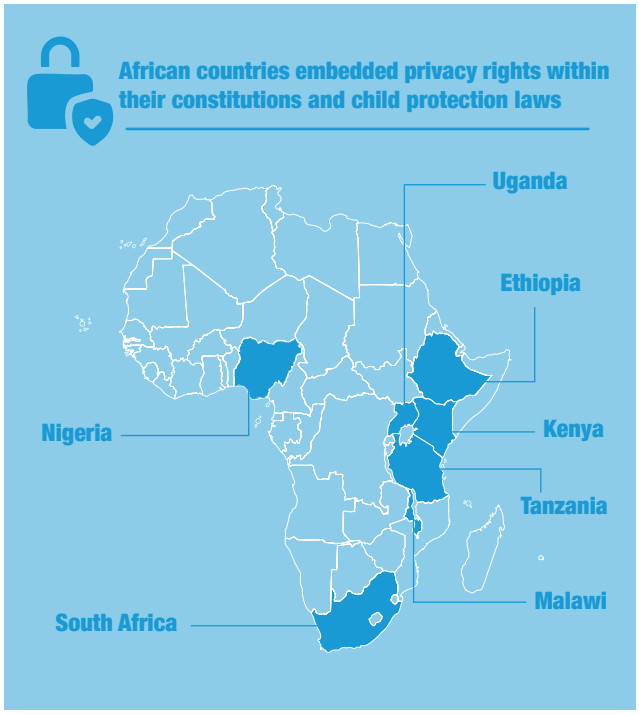
20 *African Charter on Human and Peoples' Rights, https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf*
21 *African Charter on the Rights and Welfare of the Child, https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf .*
22 *African Union Convention on Cyber-security and Personal Data Protection, "Status List," https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf*
23 *Centre for Human Rights: Pretoria University Law Press (PULP), A study on children's right to privacy in the digital sphere in the African region (2022)., supra.*
24 *The African Union Child Online Safety and Empowerment Policy, https://au.int/sites/default/files/documents/43798-doc-African_Union_Child_Online_Safety_and_Empowerment_Policy_Feb_2024.pdf*

The Digital Transformation Strategy for Africa (2020-2030) also recognises the youthful population and the children's structure of Africa and the need to invest in their digital transformation or skills as an important opportunity in the digital era. It further emphasises the inclusion of child privacy in online spaces alongside media and information literacy building.

At the East African Community level, the draft Data Governance Policy Framework does not have specific provisions on children and data governance. It only mentions children in the definition of sensitive personal data and in respect to maternal and child health data.[25] On the other hand, the Economic Community of West African States (ECOWAS) and Southern African Development Community (SADC) do not have a similar framework beyond the laws that regulate data protection.

Despite the existing international and regional frameworks, national implementation remains inconsistent and often inadequate, leading to ongoing privacy violations in the digital sphere, especially for children including wanton surveillance even on children, identity theft, fraud, phishing, scams, hacking, and blackmail. Although many African countries surveyed by this research including Nigeria, Malawi, Tanzania, Ethiopia, Kenya, South Africa and Uganda have embedded privacy rights within their constitutions and child protection laws, the development of comprehensive legislation specifically protecting children's privacy remains inadequate. Currently, 36 of Africa's 55 countries have enacted data protection laws, with considerable variation in scope and enforcement, while three have pending bills, and 10 lack legislation altogether.[26]

While international and regional frameworks provide a strong foundation for children's privacy rights, significant work remains to be done at the national level. Strengthening children's privacy rights in Africa requires effective implementation of the existing legal protections. This also calls for the adoption of comprehensive national legislation that aligns with international human rights norms and best practice, robust enforcement mechanisms, and periodic updates in line with technological advancements.



25 *According to the Policy Framework, "sensitive personal data means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject."*

26 *Mapping the progress (and delays) for data protection in Africa, https://dataprotection.africa/data-protection-in-africa-progress/.*

National Implementation, Protection and Challenges

While many African nations have enshrined privacy rights within their constitutions and other laws, specific protection of child privacy remains a major challenge. With only 36 States having specific legislation on privacy and data protection, protection of children's privacy remains a challenge. Below are selected country examples that illustrate the diverse approaches and ongoing challenges in safeguarding children's privacy rights on the continent.

East Africa

Kenya

Online violence against young people in Kenya is a major challenge, with physical, sexual and emotional violence on the increase. In 2019, the Ministry of Labour and Social Protection conducted a survey on the status of violence against children to build on its first report of 2018.[27] According to the 2018 report, a third of females and up to 18% of males in the country experienced some form of sexual violence before they attained the age of 18.[28] The 2019 report recognised online violence as a major concern that requires deeper research on the contributing factors and workable responses and solutions.

Communications Authority of Kenya recognises that children are the most vulnerable consumers in the online spaces.[29] In 2011, the Authority held a multi-stakeholder workshop themed "Protecting Children in Cyberspace: Whose responsibility is it?" that facilitated conversations on measures to secure children's privacy online.[30] Consequently, in 2015, the Authority rolled out a Child Online Protection (COP) programme.[31]

The programme brings together various stakeholders including children and their parents or guardians, who are equipped with tools on safe Internet use and how to eliminate exposure to risks and vulnerabilities.[32] The Authority further provides a self-help *online platform* where various stakeholders can engage on child safety online.[33]

The Industry Guidelines for Child Online Protection (COP) and Safety in Kenya that were issued by the Authority also provide a comprehensive framework for child safety in the digital environment.[34] They specifically target common vulnerabilities that children face including sexual exploitation and abuse, cyber harassment, cybercrimes, radicalisation, and online addiction. The guidelines apply to a wide range of stakeholders including ICT products and services providers who target children as the primary consumers. The targeted stakeholders include Application Service Providers (ASPs) and Content Service Providers (CSPs), broadcasters, mobile operators, and hardware manufacturers and vendors. The are supposed to ensure that age verifications are considered, all relevant information is provided, they package their products appropriately and adhere to all guidelines including broadcasting and relaying of information on various platforms. They are also required to report regularly on complaints received and the outcomes of complaints while consumers are encouraged to continually report all forms of non-compliance to the authority.[35]

27 *Republic of Kenya, Ministry of Labour and Social Protection "Violence Against Children Survey Report 2019," https://www.unicef.org/kenya/media/1516/file/2019%20Violence%20Against%20Children%20Survey%20(VACS)%20.pdf*

28 *United Nations Children's Emergency Fund, Centers for Disease Control and Prevention, Kenya National Bureau of Statistics. Violence against Children in Kenya: Findings from a 2010 National Survey. Summary Report on the Prevalence of Sexual, Physical and Emotional Violence, Context of Sexual Violence, and Health and Behavioral Consequences of Violence Experienced in Childhood. 2012. United Nations Children's Emergency Fund. Nairobi, Kenya.*

29 *Communications Authority of Kenya, "Child Online Protection," https://www.ca.go.ke/child-online-protection*

30 *Ibid.*

31 *Ibid.*

32 *Ibid.*

33 *Communications Authority of Kenya, "Lets's Be Safe Online," https://cop.ke-cirt.go.ke/*

34 *Communications Authority of Kenya, "Industry Guidelines For Child Online Protection and Safety," https://repository.ca.go.ke/server/api/core/bitstreams/de1c39c6-1e2d-4a69-a2c2-154d324cf627/content*

35 *Ibid.*

Kenya has also developed a National Plan of Action (NAP) to Tackle Online Child Sexual Exploitation and Abuse in Kenya 2022–2026.[36] The five-year plan that was developed by the Directorate of Children's Services aims to guide tech sector players, policymakers, civil society organisations, and communities to take measures that maximally protect children online.[37] Interventions under the NAP include legal and policy leadership and coordination; prevention through knowledge building and skilling of children, parents, guardians and caregivers; capacity building and strengthening of technical and human resources, response and support; as well as monitoring and evaluation for evidence building, tracking and documenting lessons.[38] The implementation also requires collaboration of the various stakeholders as laid down in the Industry Guidelines for Child Online Protection (COP) and Safety in Kenya.

Moreover, back in 2017, there were efforts to address the gaps in the online protection of children. The Kenya Film Classification Board (KFCB) convened a Child Online Safety Retreat for stakeholders including Internet Service Providers (ISPs) and other organisations like the Kenya Network Information Centre (KeNIC) and the ICT Authority to deliberate on ways to protect children from harmful online content including sexual exploitation, violence, self-harm and pornography.[39] The convening birthed the NAP and the Industry Guidelines for Child Online Protection.

In terms of laws, the Computer Misuse and Cybercrimes Act, 2018, addresses cybercrimes including violence against children. It further criminalises child pornography under section 24, online child grooming and the dissemination of harmful content to minors. Under section 24, a conviction for child pornography attracts a fine not exceeding KES 20 million (USD 154,452) or imprisonment for a term not exceeding 25 years, or both. Similarly, section 16 of the Sexual Offences Act, 2011 provides for, and penalises the offence of child pornography. Furthermore, section 16A of the Sexual Offences Act prohibits and penalises communication of sexual nature content with a child. Upon conviction, a perpetrator is liable to less than KES 500,000 (USD 3,861) or imprisonment for a term of not less than five years, or to both.

Conviction for child pornography attracts a fine not exceeding **KES 20 million** or imprisonment for a term not exceeding **25 years**, or **both.**

The Data Protection Act, 2019 also provides for the protection and safeguard of children's data privacy. Under section 2, data relating to children is considered sensitive personal data and under section 33, processing of personal data relating to children must be subjected to consent of parents or guardians. However, data protection including for the protection of children remains a major challenge with data protection considered wanting in providing robust protection.

36 *National Plan of Action to Tackle Online Child Sexual Exploitation and Abuse in Kenya 2022–2026, https://www.nccs.go.ke/sites/default/files/resources/National-Plan-of-Action-to-Tackle-Online-Child-Sexual-Exploitation-and-Abuse-in-Kenya-2022-2026.pdf*

37 *Ibid.*

38 *Ibid.*

39 *Kenya Film Classification Board (KFCB), "Child Online Safety Retreat 1st to 3rd June 2017 Report," https://kfcb.go.ke/sites/default/files/2021-01/KFCB-Child-Online-Safety-Report.pdf*

Rwanda

In its third periodic report on the implementation of the African Charter on the Rights and Welfare of the Child, the government provided a detailed account of legal policy and institutional frameworks and progress on the implementation of the provisions of the charter including in child protection. The report highlights the progressive measures undertaken at the national level to address child protection, including the adoption of laws, increased budget allocations for child care and welfare, education and healthcare access, and efforts to address specific vulnerabilities in children such as those in refugee communities and those in conflict with the law - including sexual violence and exploitation, child pornography, grooming and recruitment andemotional violence.

The Rwanda Child Online Protection Policy was issued by the Ministry of ICT and Innovation in 2019.[40] The policy recognises children's vulnerability to online violence and identifies strategies to mitigate risks, threats and harms associated with the use of digital technologies by children. The obligation to mitigate risks and harms and the general implementation of the policy is placed on a number of institutions including government and public agencies; information and communications technology companies (including hardware and infrastructure companies); telecommunication companies; communities and civil society organisations; parents, teachers and children themselves.[41]

The Policy proposes the establishment of a governance framework to act as a central point for the direction and coordination of all policy areas. It is based on regional and international standards such as the CRC, *World Summit on the Information Society's* (WSIS) *Outcomes Document and Tunis Commitment on the role of ICTs in child development*, *UN Sustainable Development Goals* (SDGs), *the International Telecommunication Union (ITU)'s COP Guidelines* which seek to establish a safe and secure digital environment for children, the *WeProtect Global Alliance's Model National Response* that seeks to address online sexual exploitation and abuse, the *ACRWC* and the *African Youth Charter* (AYC).

In 2024, Rwanda issued a Ministerial Order (the Order), which outlines the obligations of service providers in protecting children online.[42] The Order aims to promote the safety and protection of children while accessing online content, to protect them against harmful content and to raise awareness about parental control over child online activities and content filtering tools. The scope of application of the Order is wide as it extends to persons or organisations who broadcast or provide content online or provide access to online content. The specific parties to be held to account include digital content providers, ISPs, cybercafés and public Wi-Fi access providers, broadcasters and TV service providers operating online, social media users and YouTubers, and parents, teachers, guardians, and caregivers.[43] These stakeholders must undertake all measures to address the protection of children while using digital technologies. This Order demonstrates a higher-level commitment to create a safe online environment for children.

40 Rwanda Child Online Protection Policy, https://rura.rw/fileadmin/Documents/ICT/Laws/Rwanda_Child_Online_Protection_Policy.pdf
41 Ibid.
42 Ministerial Instructions N° 001/MINICT/2024 of 22/01/2024, https://www.minijust.gov.rw/index.php?eID=dumpFile&t=f&f=91546&token=d5eb7096a06042554606ab1c4fac9b87b9de3c2e
43 Ibid.

The specific laws that have some bearing on online protection of children include the Law N°71/2018 of 31/08/2018 Relating to the Protection of the Child, which provides a framework for the protection of children. It for instance prohibits child pornography and all forms of sexual exploitation of children.[44] Article 33 prohibits showing of pornographic images and sounds to children. Conviction under this article attracts imprisonment for a term of not less than five years and not more than seven years with a fine of not less than three million Rwandan francs (USD 2,133) and not more than FRW five million (USD3,556). Article 34 prohibits recording of a child's pornographic picture or voice, and upon conviction, one may be liable to imprisonment for a term of not less than five years and not more than seven years and a fine of not less than seven million Rwandan francs and not more than FRW 10 million (USD 6,928). Article 35 prohibits advertising of children pornographic images, and those convicted may be liable to imprisonment for a term of not less than five years but not more than seven years and a fine of not less than FRW 15 million (USD 10,392) and not more than FRW 20 million (USD 13,855).

Article 33 prohibits showing of pornographic images and sounds to children. Conviction under this article attracts imprisonment for a term of not less than **five years** and not more than **seven years** with a fine of not less than **three million Rwandan francs (USD 2,133)** and not more than **FRW five million (USD3,556)**.

According to article 9 of the law, processing of a child's personal data requires parental consent which must also be in the interest of the child. The only exception arises where such data processing is for protecting the vital interests of the child. [45]

Despite the extensive multi-stakeholder approaches, gaps in implementation, enforcement, limited digital literacy and awareness, increased online threats, risks and crimes have continually degraded the enforcement of the legal and policy frameworks.[46]

44 *Law N°71/2018 of 31/08/2018 Relating to the Protection of the Child, https://www.refworld.org/sites/default/files/legacy-pdf/en/2018-9/6087404d4.pdf*
45 *Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy, https://www.risa.gov.rw/data-protection-and-privacy-law*
46 *Edith Luhanga, "Applications for Rwandan Children's Online Safety," Carnegie Mellon University Africa, https://www.africa.engineering.cmu.edu/projects/online-safety.html*

Uganda

Uganda does not have a specific law on child online protection. However, a number of laws offer guidelines on their protection. These include the Constitution of the Republic of Uganda, 1995 and the Children Act Cap. 62. The Constitution of the Republic of Uganda in article 27 protects the right to privacy for all citizens including children. Similarly, sections 4(1)(g) and 148(1) of the Children Act guarantee the right to privacy as a right across all fronts including during court proceedings and publication of content. Furthermore, section 1 of the Children Act defines child exploitation to include child pornography and section 9 strictly prohibits child sexual exploitation and abuse, including the use of children in pornographic performances.

Additionally, a set of cyber laws such as the Data Protection and Privacy Act Cap. 97, the Electronic Transactions Act Cap 98 and the Computer Misuse Act, 2011 offer some basic protection in the online spaces. During the COVID-19 pandemic, school closures led to increased internet access among children, exposing them to risks such as online exploitation and predation.

The Uganda Communications Commission (UCC), which is one of the key stakeholders, is enjoined to promote children's internet safety through campaigns and outreach, as well as to advocate for financing of safe internet initiatives. The UCC, through the Computer Emergency Response Team (CERT), is tasked with overseeing this, aiming to restrict such material and prosecute offenders. In 2020, UCC published a survey report on Children's Online which emphasises the need for widespread awareness campaigns and resources to help children and parents understand and respond to cyber threats.[47] This includes empowering children to recognise and report suspicious or harmful behaviour. And ISPs[48] are encouraged to offer parental control tools and restrict access to inappropriate content, and to support parents in creating safer online environments.[49]

A 2020 report published by UCC highlights aspects of protection against threats to child privacy and safety online across various sections with particular emphasis on awareness creation efforts, parental controls, and regulatory measures.[50] The report encourages open communication, enabling children to report harmful interactions, and promoting responsible online behaviour.[51] The report highlights the need to protect children from online risks including increasing awareness efforts and providing channels for reporting cyber threats.[52] It provides guidance to parents and guardians to effectively monitor and control children's internet usage with specific instructions such as installing parental controls, setting time limits, and monitoring online activities.[53] As part of the control measures, it emphasises collaborations with national and international agencies to monitor, restrict, and block harmful content, as well as efforts to trace origins for prosecution.

47 *UCC's Final Report on Ugandan Children's Online Survey 2020, https://www.ucc.co.ug/wp-content/uploads/2023/10/Final_Report_Child-Online-Survey.pdf.*
48 *Ibid., pages 80 - 82.*
49 *Ibid.*
50 *Ibid., pages 80 - 82*
51 *Ibid.*
52 *Ibid.*
53 *Ibid.*

Online child sexual exploitation and abuse (OCSEA) is another issue of concern. A 2021 report by SafeOnline found that around 40% of Ugandan children aged 12–17 using the internet, are exposed to online exploitation including requests for sexual content or being threatened online. Notably, most perpetrators were people that the affected children know, and social media platforms like Facebook, Messenger, and WhatsApp are frequently used as platforms for such exploitation. Sadly, many children do not report exploitation incidents due to lack of awareness, stigma, fear of victim-blaming, and distrust in law enforcement. Only a small percentage report to authorities, often facing additional challenges like informal payment demands. [54]

According to the National IT Survey Report of 2022 by the National Information Technology Authority, Uganda (NITA – U), parental awareness of children's potential online victimisation was relatively low, with 88.3% of parents admitting they were unsure if their child had experienced any online threats, such as cyberbullying or exposure to harmful content.[55] Furthermore, 55.3% of parents reported that they did not take specific actions to safeguard their children online, indicating a significant awareness and action gap regarding online safety.[56] While children's internet access and online activities are moderate, the low parental engagement in monitoring and safeguarding measures highlights an urgent need for increased awareness and education on online safety measures. The findings underscore the need for civic programmes that educate both children and parents about internet safety to foster a secure digital environment.

The Electronic Transactions Act Cap 98 facilitates electronic communication and transactions while ensuring the protection of consumers, including minors, in the digital environment. The Data Protection and Privacy Act, which is the primary legislation regulating the collection, processing, and storage of personal data, addresses data protection. Under section 8, collection and processing of personal data of children may only be done subject to the consent of the parent or guardian or any other person having authority to make decisions on behalf of the child.

The Computer Misuse Act Cap 96, which criminalises unauthorised access, interception, and misuse of electronic data is an instructive piece on children's protection online. Section 22 prohibits child pornography and any associated acts. Upon conviction, one is liable to a fine not exceeding UGX 7,200,000 (USD 1,965) or to imprisonment for a term not exceeding 15 years, or both. On the other hand, section 23 prohibits sending, sharing or transmitting any information about or that relates to a child through a computer without the consent of the parents or guardians, except where such action is done with authority under the law or in the best interests of the child. A conviction under this section attracts a fine not exceeding UGX 15,000,000 (USD 4,093) or imprisonment for a term not exceeding seven years, or both.

Unauthorised access, interception, and misuse of electronic data is an instructive piece on children's protection online. Section 22 prohibits child pornography and any associated acts.Upon conviction, one is liable to a fine not exceeding **UGX 7,200,000 (USD 1,965)** or to imprisonment for a term not exceeding **15 years**, or **both**

54 *2021 "Disrupting Harm in Uganda" brief, https://safeonline.global/wp-content/uploads/2023/12/DH-Uganda-brief.pdf.*
55 *The National IT Survey Report 2022, https://www.nita.go.ug/sites/default/files/2022-12/National%20IT%20Survey%20Report%202022%20-%20Final.pd*
56 *The National IT Survey Report 2022, page 87*

The Uganda National Child Policy, 2020 makes strides to give specific protections for children against online risks. It addresses the increase in online child sexual exploitation, noting the rise of cases like child sexual abuse/exploitation material. It highlights the increase in online risks due to more internet usage among children, especially with shifts like COVID-19-induced online schooling.[57] Under the policy framework, it mentions emerging challenges affecting children, such as online child sexual abuse and exploitation. Objectives of the policy include protecting children from all forms of violence, abuse, neglect, and exploitation, covering digital forms of abuse.

Despite these legal provisions, the enforcement of the laws and policies by agencies like the UCC and law enforcement bodies has been ineffective. Challenges such as limited technical capacity, inadequate resources, and low levels of digital literacy among the public hinder the effective implementation of these laws. The UCC has initiated programmes to educate stakeholders, but the reach and impact of these initiatives require enhancement.

Law enforcement agencies, particularly the Directorate of Forensic Services of the Uganda Police Force which is responsible for detecting, investigating and preventing crime regarding highly specialized areas including cyber crimes.[58] However, the Directorate faces obstacles such as technological limitations and the anonymous nature of the internet, which complicates investigations.

Civil society organisations are also contributing to protecting children online. For instance, the Internet Society of Uganda (ISOC) developed an *Online Safety Education Toolkit* that is useful and convenient for young children and youth between ages of five and 20 years to prevent online victimisation by teaching them how to stay safer online and offline.[59] While this is a useful tool for educational purposes, there is a need to disseminate it widely across academic institutions to equip learners on the relevant protective measures to strengthen their digital security.

The judiciary plays a crucial role in interpreting and enforcing laws related to online child privacy. The judiciary has for instance installed modern audio-visual technology that protects child victims and witnesses when giving evidence especially in sexual abuse cases.[60] This is one of the fundamental steps despite shortfalls in decisive dealing with online child privacy violations in the country.

The existing legal and policy frameworks in Uganda provide a solid foundation for protecting children's online privacy. However, implementation gaps persist. The rise in online threats, as evidenced by recent statistics,[61] indicates that children remain vulnerable especially to online sexual exploitation and abuse.[62] Factors such as limited resources for enforcement agencies, insufficient public awareness, and rapid technological advancements contribute to the gap between legislation and actual protection. Strengthening inter-agency collaboration, enhancing capacity building, and increasing public education on online risks are essential steps toward improving the effectiveness of protections against online threats to children in Uganda.

57 *Uganda National Child Policy, https://docs.africhild.cloud/index.php/s/EfAMgA8B56cGB2i , Page 3,*

58 *Directorate of Forensic Services, https://upf.go.ug/directorate/*

59 *Online Safety Education Toolkit for Young People in Uganda, https://demo.nita.go.ug/sites/default/files/2024-06/COP-Toolkit-ISOC-UG%281%29.pdf*

60 *Moses Sserwanga, "UNICEF boosts Uganda's justice system to protect victims, survivors and alleged child offenders" UNICEF, 17 May 2023, https://www.unicef.org/uganda/stories/unicef-boosts-ugandas-justice-system-protect-victims-survivors-and-alleged-child-offenders*

61 *ECPAT International, INTERPOL and UNICEF, Disrupting Harm in Uganda: Evidence on online child sexual exploitation and abuse (ECPAT, INTERPOL, UNICEF 2021).*

62 *ECPAT International, INTERPOL and UNICEF, Protecting Uganda's Children from Online Sexual Exploitation and Abuse: The Way Forward (Safe Online 2021) https://safeonline.global/wp-content/uploads/2023/12/DH-Uganda-brief.pdf accessed 16 June 2025.*

The United Republic of Tanzania

Tanzania faces similar challenges like the rest of Africa in dealing with child protection online. Sexual exploitation and abuse, cyber bullying and harassment, grooming, sex predation, trafficking and emotional abuse are common challenges.

The Constitution of Tanzania in article 16 guarantees the right to privacy and personal security. The Personal Data Protection Act, 2023 guarantees the privacy and protection of personal data.[63] The Cybercrimes Act addresses cybercrimes including the penalisation of child pornography under section 13. According to section 3, child pornography means pornographic material that depicts presents or represents: (a) a child engaged in a sexually explicit conduct; (b) a person appearing to be a child engaged in a sexually explicit conduct; or (c) an image representing a child engaged in a sexually explicit conduct. Under section 13, a person who contravenes subsection (1) commits an offence and is liable on conviction, to a fine of not less than TZS 50 million (USD 5,655) or three times the value of undue advantage received, whichever is greater, or to imprisonment for a term of not less than seven years or to both. The convict may in addition to any other punishment, be ordered to compensate a person injured by the offence.

Other laws that have a bearing on child protection in online spaces include the Electronic Transactions Act, 2015 which provides a framework for regulating electronic transactions and communications. This law may also be interpreted to include children. Similarly, the Law of the Child Act, 2019, which is dedicated to protecting children including their rights, can be interpreted to include protection against online harms.[64] This Act under section 83, prohibits sexual exploitation of children. This exploitation extends to inducement and coercion, prostitution and unlawful sexual practices and child pornography. The penalty on conviction for the offences is a fine of not less than TZS one million (USD 377) and not more than TZS 500 million (USD 186,008) or imprisonment for a term of not less than one year and not more than 20 years or to both. Furthermore, section 158(1) on general prohibition among others bars the publication, production, shows or causing the publication, production or showing a photograph or a picture of a child or a dead child containing brutal violence or in a pornographic posture; and the publication of any information which is prejudicial to the best interest of a child.

The Tanzania Communications Regulatory Authority (TCRA) has a number of regulations which regulate the communications sector and provide direction on broadcasting of content and filtering of content online to ensure that any issues such as potential harms to children are addressed. For instance, the Electronic and Postal Communications (Online Content) Regulations, 2020 as amended 2022 under regulation 18 extend the obligation of child protection to online content service providers. Hence, "[A]n online content service licensee, host or online content user shall take measures to ensure children are protected against access to any content that is harmful to the children's wellbeing."

While Tanzania has made legislative strides to deal with child safety and protection online, children remain widely exposed to online harms due to advancing technologies. This is further worsened by weak enforcement of laws, high digital illiteracy rates, limited and inadequate capacities in enforcing rights in the online spaces.

63 *Personal Data Protection Act, 2023, https://www.pdpc.go.tz/media/media/THE_PERSONAL_DATA_PROTECTION_ACT.pdf*
64 *Law of the Child Act, 2019, http://parliament.go.tz/polis/uploads/bills/acts/1452143878-ActNo-21-2009.pdf*

North Africa

Algeria

Algeria's Law No. 18-07 relating to the Protection of Individuals in the Processing of Personal Data entered into force on August 10, 2023.[65] The framework regulates the processing of personal data, including the requirement for the data subject to provide consent. The law further recognises the right of children to require consent from a parent to process their data. It also gives power to the judge to override the consent granted by the parents.[66]

With a population of 46 million people in 2024, Algeria had 33.49 million internet users in the first quarter of 2024, the equivalent of 72.9% of the total population.[67] With the increase of internet users, the adoption of a data protection law was a step in the right direction in the protection of the right to privacy. In August 2023, the establishment of the National Data Protection Authority strengthened data protection.[68]

Algeria has enacted Law 18-07 of 25 Ramadhan 1439 which addresses children's right to privacy. This law provides that the primary requirement for processing children's data is to obtain consent from a legal representative or a competent court.[69]

Other laws that impact on child protection online include the Algerian Penal Code of 1971 as amended which contains provisions on the protection of children. Amongst the key provisions are those that seek to address sexual exploitation of minors, corruption of minors and the production of child pornography. Similarly, the Law No. 09-04 relating to the rules specific to the protection of children protects children from online harms. The Ministry of Post and Telecommunications has also issued a Practical Guide to Protecting Children on the Internet.[70] This guide sets benchmarks for online safety. In addition, the National Strategy for Cybersecurity provides for measures necessary for the protection of children online.[71]

Despite the existing legal protection, the law does not sufficiently address child privacy issues. Children in Algeria from the age of 10 have been reported as users of mobile phones.[72] Though children tend to use phones for socialising and educational purposes, there is a prevailing risk of online sexual abuse, cyberbullying, among others, but with inadequate legal protection which fall short of the international human rights standards.

Children from the age of

10

have been reported as users of mobile phones

65 *Data Guidance, "Algeria," https://www.dataguidance.com/jurisdictions/algeria*
66 *Data Protection Africa, "Algeria Data Protection Factsheet," https://dataprotection.africa/algeria/*
67 *International Trade Administration, "Algeria Country Commercial Guide," 2024-09-19, https://www.trade.gov/country-commercial-guides/algeria-digital-economy*
68 *DLA PIPER, "National data protection authority in Algeria," https://www.dlapiperdataprotection.com/?t=authority&c=DZ#insight*
69 *Centre for Human Rights: Pretoria University Law Press (PULP), A study on children's right to privacy in the digital sphere in the African region (2022)., supra.*
70 *Practical Guide For Parents, Guardians And Educators To Protect Children Online, https://www.mpt.gov.dz/wp-content/uploads/2023/12/guide-pratique-protection-des-enfants-en-ligne.pdf*
71 *See for instance, Oualid Mortadha Naoua, Cybersecurity Strategy in Light of Digital Transformation for Algerian Institutions, https://eelet.org.uk/index.php/journal/article/download/2188/1967/2399*
72 *Guedjali, A., & Benghebrid, R. (2024). The use of smartphones among young people . Marketing Science & Inspirations, 19(1), 26–38, https://doi.org/10.46286/msi.2024.19.1.3*

Egypt

Egypt is one of the countries that has taken progressive steps aimed at protecting children's right to privacy in the digital era by enacting enabling legal frameworks. The right to privacy including for children in Egypt has been protected in its Constitution since 1923.[73] The newly adopted Constitution following the referendum in January 2014 guarantees the right to privacy in article 57.[74] The right extends to children as well.

In 2020, the government of Egypt adopted a legal framework that protects the right to privacy and personal data. The law in article 1 defines sensitive personal data to include data relating to children. Under article 12, if sensitive personal data relating to children is to be processed, the legal guardian's consent must be obtained.

Egypt's Cybercrime Law No. 175 of 2018 aims to address online crimes including crimes perpetrated against children. The law criminalises all forms of child pornography, cyber bullying and online harassment and the use of information networks to endanger children. This is very pertinent since the 2017 Central Agency for Public Mobilization and Statistics report revealed that 46.9% of children aged 4-17 use mobile phones while 80.6% of this percentage are aged 15-17. [75]

46.9%
Children aged **4-17** use mobile phones

80.6%
are aged 15-17

Similarly, Law 12 of 1996, amended by Law 126 of 2008 (the Child Law) provides for a comprehensive framework for child protection. It specifically prohibits abuse and exploitation which often manifests in the publication of children's data either in the form of audio or visual for purposes such as pornography, sexual exploitation, and defamation.[76] Under article 96, a child is considered to be at risk if exposed "…in the family, school, care institutions, or other to violence, or to acts contrary to public morals, or pornographic material, or to commercial exploitation of children, or to harassment or sexual exploitation, or to the illegal use of alcohol or narcotic substances affecting the mental state.."[77]

The National Council for Childhood and Motherhood (NCCM), which was established in 1988 by Presidential Decree number 54 of 1988, later amended by Presidential Decree number 273/1988 and Presidential Decree number 28/2011, is critical in child protection as it coordinates the implementation of child protection including of policies in the online spaces.[78]

The Ministry of Communications and Information Technology (MCIT) is an important agency in ensuring online protection and safety of children. It is charged with the implementation of the national cybersecurity strategy by adopting policies and programmes on protecting citizens including children in the online spaces.[79] Through its digital literacy and safe internet usage, families and children are crucially empowered to navigate common child safety challenges online in order to keep safe in the online spaces.[80] The MCIT also collaborates with international organisations to transform the impact of ICT usage by children such as through the development of use guidelines while also ensuring its safe usage online.[81]

74 *Privacy International, "State of Privacy Egypt," https://privacyinternational.org/state-privacy/1001/state-privacy-egypt*
75 *Constitution of Egypt 2014, https://www.constituteproject.org/constitution/Egypt_2014.pdf*
76 *Central Agency for Public Mobilization and Statistics (Egypt), Report on Mobile Phone and Internet Usage (20 November 2017)*
77 *Law No. 12 of 1996 Promulgating the Child Law Amended by Law No. 126 of 2008, https://www.refworld.org/legal/legislation/natlegbod/1996/en/119718*
78 *Ibid.*
79 *The National Council for Childhood and Motherhood, https://hrightsstudies.sis.gov.eg/en/bodies/councils/local/the-national-council-for-childhood-and-motherhood/*
80 *Cyberwellness Profile Egypt, https://ictpolicyafrica.org/api/documents/download?_id=5d80705a1c3577001bda4005*
thraDigitalWellbeing, Country Report: Egypt, 2024, https://dwi-api.ithra.com/uploads/Egypt_country_profile_92195c33f1.pdf
81 *Ministry of Communications and Information Technology, UNICEF Sign Cooperation Protocol to Empower Children with Disabilities, 31 August, 2018,*
https://www.unicef.org/egypt/press-releases/ministry-communications-and-information-technology-unicef-sign-cooperation-protocol

Southern Africa

Botswana

The Constitution of the Republic of Botswana provides for the right to privacy under section 9 of every person in Botswana.[82]

The Children Act, 2009 provides a comprehensive framework for the protection of children and the enjoyment of their rights.[83] As any other law on children rights, the best interests of the child are fronted in line with the international standards on the protection of children. Section 20 of the Act protects the right to freedom of expression of every child. However, the right to freedom of expression is exercised in line with the child's best interests. The section also emphasises the need for parental guidance and to protect the child from pornography and other influences which may cause emotional, physical, psychological or moral harm to the child. Furthermore, section 58 protects children against involvement in acts of pornography. The law further prohibits the storing, keeping or distributing of any indecent images of a child depicting any form of illegal sexual activity against a child.

The Data Protection Act, 2024 which replaced the Data Protection Act of 2018 provides for data protection and imposes more stringent requirements on data controllers and processors to comply with data protection standards.[84] The Act, among others, in section 26 provides for the conditions for lawful processing of personal data. Under section 26(f), processing is necessary for legitimate purposes by data controllers or third parties save where the data subject is a child. Under section 29, where processing of personal data of a child relates to the offer of information society services and, the data subject is a child below 16 years of age, consent must be sought from a person with parental responsibility over the child.

The Cybercrime and Computer Related Crimes Act, 2018 in section 19 (1) (a-c) and (2 (a-e) prohibits pornographic or obscene material in which children may be engaged including in creation, portraying, publishing, accessing or possessing of content. The prescribed penalty on conviction is up to fine not exceeding BWP 100,000 (USD 7,494.1), or to imprisonment for a term not exceeding five years, or to both.

Penalty on conviction is up to fine not exceeding **BWP 100,000 (USD 7,494.1)**, or to imprisonment for a term not exceeding **five years**, or **both**.

Further, under section 19(3)(a), a person who, by means of a computer or computer system, communicates with a person who is, or who the accused believes is under the age of 18 years, for the purpose of facilitating the commission of the offence of child pornography, or the offences of prostitution, rape or indecent assault under the Penal Code shall on conviction be liable to a fine not exceeding BWP 100,000 (USD 7,494.1), or to imprisonment for a term not exceeding five years, or to both.

The law further provides for deletion and destruction orders by the Director of Public Prosecutions or any authorised person under section 29 in respect of data in a computer or computer system or other information communication technology medium which contains pornography, obscene material or child pornography.

The Communications Regulatory Authority Act, 2012 under section 37 requires licensees, where a programme to be broadcast or re-broadcast is not suitable to be exhibited to children, advise or warn members of the public accordingly. This protects children against harmful content.

82 *Constitution of the Republic of Botswana, 1966, https://www.parliament.gov.bw/images/constitution.pdf*
83 *The Children Act, 2009, http://jafbase.fr/docAfrique/Botswana/Children%20act.pdf*
84 *Data Protection Act, 2024, https://itlawco.com/wp-content/uploads/2025/01/botswana-data.protection.act_.2024-website-copy.pdf*

Child safety and protection in the online spaces of Botswana's presents several issues. While there are laws that make strides in addressing the needs, rights and safety of children through prescription and engagement of stakeholders, implementation remains challenging especially in underserved communities that grapple with lack of relevant skills and knowledge, digital illiteracy and digital exclusion and the upsurge of online crimes. Like other countries on the continent, there is a need to bridge the digital divide, raise awareness and enhance capacities of the public and children in child protection and safety online and to take measures aimed at enforcing the protective laws.

South Africa

The Constitution of the Republic of South Africa in section 14 guarantees the right to privacy including for the children. Section 28 provides that a child's best interests are of paramount importance in every matter concerning the child. This essentially extends into issues regarding protection of children in the online spaces.

The Department of Communications and Digital Technologies which is established by the SITA Act, 1998 (Act 88 of. 1998) takes a holistic approach to protecting individuals including children in the online space. It works on addressing cybersecurity by, among others, ensuring that stakeholders undertake legal, policy and technical steps to tackle online crimes, issues and challenges.[85]

South Africa's Protection of Personal Information Act (POPIA) 2013 stands out as one of Africa's most advanced privacy laws, offering a comprehensive framework for safeguarding personal information, including that of children. Under sections 34 and 35, POPIA regulates data collection, storage, and usage, aiming to protect minors from privacy risks by putting in place the necessary checks prior to Processing of personal information of children. Therefore, under section 34, A responsible party may only process personal information concerning a child subject to the specifications set out in section 35 including necessity, consent, historical and statistical research, and publicly exposed information justifications among others.

The Cybercrimes Act No. 19 of 2020 and the Sexual Offences and Related Matters Act address cybercrimes broadly including those committed against children. Both Acts prohibit sexual violence against children including sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, child pornography and using children for pornographic purposes or benefiting from child pornography.[86] The Sexual Offences law spells out a wide range of acts of a sexual nature that could potentially victimise children.

Despite these legal protections, enforcement remains a challenge. In 2020, a girl child in South Africa received anonymous threats, including threats of gang rape and murder, through Instagram. Seeking to protect her safety, the girl and her family attempted to identify the perpetrator. This effort led them into a complex international legal process aimed at compelling Facebook to disclose the identity associated with the Instagram accounts responsible for the threats. The difficulty in compelling Facebook, a U.S.-based company, to disclose information about an Instagram user to a South African complainant highlights several gaps in legislation concerning digital privacy, international jurisdiction, and social media accountability.[87] Additionally, cyberbullying and unauthorised data usage continue to affect South African children, with a 2022 UNICEF report indicating that 34% of children experienced cyberbullying and lacked knowledge on data privacy.[88]

Despite several efforts to put in place laws and several policies aimed at preventing and addressing cyberbullying from the Cybercrimes and Cybersecurity Bill enforced in 2018, the National Cybersecurity Policy Framework launched by the Department of Communications and Digital Technologies in 2020, to the Department of Basic Education's policies to address cyberbullying in schools, the lack of stringent laws and limited public awareness continues to exacerbate this issue, making it a widespread problem.[89] These challenges are hard to curb due to the evolving nature of technology, which presents new challenges of dealing with online crime against children. These developments and challenges require deliberately calculated efforts that seek to primarily buttress child protection and safety online.

85 *Department of Communications and Digital Technologies, "Child Online Protection (COP)," https://www.dcdt.gov.za/single-article/78-jm-sample-data/303-programme-8-child-online-protection*

86 *See Schedule to (Section 58) of the Cybercrimes Act No. 19 of 2020, https://media.lawlibrary.org.za/media/legislation/498/source_file/2020-19.pdf and Chapter 2 Part 3 and Chapter 3 parts 1, 2 and 3 of the Sexual Offences and Related Matters Act https://www.gov.za/sites/default/files/gcis_document/201409/a32-070.pdf .*

87 *Centre for Human Rights: Pretoria University Law Press (PULP), A study on children's right to privacy in the digital sphere in the African region (2022)., supra.*

88 *ECPAT, INTERPOL, and UNICEF, 'Disrupting Harm in South Africa: Evidence on Online Child Sexual Exploitation and Abuse. Global Partnership to End Violence against Children' (2022). Accessible here.*

89 *Ntsaluba, N. (2017). The cyber security legislative and policy framework in South Africa (Master's thesis, University of Pretoria (South Africa)), https://repository.up.ac.za/bitstream/handle/2263/65706/Ntsaluba_Secutiry_2018.pdf?sequence=1*

West Africa

Ghana

Ghana faces major challenges in child privacy and safety online. Children in both urban and rural areas frequently use social media platforms where personal data is harvested and shared with third parties, often without informed consent. The vulnerable nature of children coupled with low digital literacy exacerbates their vulnerability to online exploitation. As indicated in the other countries, Ghana has been working to address child safety online.

In 2018, the Department of Children, Ministry of Gender Children and Social Protection and UNICEF Ghana produced a position paper on children's online safety concerns in Ghana.[90] The paper highlights the concerns and the policy and legal challenges in children's online safety. Amongst the highlighted risks children are exposed are pornography, online scams and fraud, cyberbullying, grooming, sexual abuse, sexual exploitation, emotional abuse, self-harm, sexting and online gaming and addiction. The paper calls upon various stakeholders including the government and the technology sector to adopt and implement measures that ensure children's safety online.

Laws that address child safety online include the Electronic Transaction Act, 2008 which defines a child as one below 18 years but does not provide clear guidelines on protection of children against sexually explicit content. The Children's Act equally lacks clear protection guarantees for children against online harms and crimes. The Data Protection Act of 2012[91] under section 37 offers foundational privacy protections against processing of children's personal data except where consent of their parents, caregivers or guardians has been obtained. However, implementation of these laws remains weak with multiple legislative gaps, and critical enforcement failure coupled with society challenges.

The 1992 Constitution in article 18(2) provides for the fundamental right to privacy.[92] The Children Act (Act 851) provides for the right to privacy of the child and emphasises the need to respect it throughout the proceedings of Family Tribunals. It further makes it an offence for any person to "publish any information that may lead to the identification of a child in any matter before a Family Tribunal except with the permission of the Family Tribunal.

In 2020, Ghana enacted the Cybersecurity Act (Act 1038) which among others criminalises sharing indecent images and photographs of a child (section 62), sexual abuse (sections 63 and 64), cyberstalking (section 65) and sexual extortion (section 66). The Act also establishes the Cyber Security Authority in section 2, which in section 4(j) is charged with promoting the protection of children online. [93]

90 *Department of Children, Ministry of Gender Children and Social Protection (2018), "Children's online safety concerns in Ghana: A position paper on legislative and policy gaps," https://www.unicef.org/ghana/media/1806/file/Child%20Online%20Safety%20-%20Legislation%20and%20Policy%20Gaps.pdf*

91 *Data Protection Act of 2012, https://nca.org.gh/wp-content/uploads/2020/09/Data-Protection-Act-2012.pdf*

92 *The Constitution of the Republic of Ghana, 1992, http://aanma.gov.gh/documents/1992%20Constitution%20of%20Ghana.pdf*

93 *Cybersecurity Act, 2020 (Act 1038), https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf*

In 2024, Ghana developed the National Child Online Protection Framework (NCOPF)[94] in line with the Cybersecurity Act, 2020 (Act 1038), the UN CRC General Comment 25, the 2020 version of ITU Guidelines and, the WeProtect Global Alliance Model National Response (MNR). The main goal of the NCOPF is to ensure a secure, responsible, and sustainable cyberspace that encourages the participation, protection, and promotion of digital literacy among children. The NCOPF serves as the central hub for all the stakeholders under the NCOPF participants to guide the implementation. The key stakeholders under the NCOPF include government entities, industry stakeholders, CSOs, educators, and various other parties involved. Within the NCOPF framework, strategies have been designed to confront the shame and stigma experienced by victims and survivors through advocacy, raising awareness, and educational efforts. Since the NCOPF recognises that children face various online risks, including sexual abuse and exploitation, online harassment, cyberstalking, and cyberbullying, the successful implementation of the NCOPF will ensure the successful online protection of children in the country.

The constitution, Data Protection Act and the Children's Act offer protections for the fundamental right of privacy including in handling of personal data relating to children including in judicial and welfare contexts. However, the laws face sophisticated methods employed by the business sector especially companies, online crime and violence, weak enforcement of the laws with inadequate response mechanisms, limited resources for enforcement and limited awareness and literacy on data rights.

94 National Child Online Protection Framework ((NCOPF), https://www.csa.gov.gh/resources/National%20COP%20Framework.pdf

Nigeria

Nigeria has a burgeoning digital economy which comes with multifaceted child protection issues. The technological issues come along with far-reaching consequences for children. The Constitution of the Federal Republic of Nigeria provides for the right to privacy in section 37. Furthermore, section 17(3)(f) protects children against any exploitation whatsoever, and against moral and material neglect.

The Child Rights Act, 2003 recognises children as a vulnerable group and elaborates their rights and obligations.[95] The Act is section 35 criminalises the importation of harmful publications. On conviction, the liability is to a fine of NGN 30,000 (USD 19.6) or imprisonment for a term of three years or to both such fine and imprisonment. The law, however, falls short of the prohibition of exploitation and online dissemination of harmful content to children.

The Nigeria Data Protection Regulation (NDPR) developed in 2019 by the National Information Technology Development Agency (NITDA) provides a regulatory framework, yet enforcement is limited, especially concerning children's privacy. The regulation aims to safeguard privacy and data rights of individuals. Article 2.4 specifies that no consent shall be sought, given or accepted in any circumstance that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts. Under article 3.1, data controllers are expected to take appropriate measures and provide any information relating to processing to the data subject, including children, in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The Nigeria Data Protection Regulation 2019: Implementation Framework published in 2020 provides guidelines on appropriate handling of personal data.[96] Section 5.5 calls on data controllers and processors to ensure that privacy policies are made in a child friendly form to enable children and their guardians to have a clear understanding of the data processing activity before grant of consent. A child under this framework is any person below 13 years.

The White Paper on the Framework for an Online Harms Protection Bill in Nigeria of 2024 recognised that Nigeria is exposed to online threats that endanger children.[97] The paper aims to provide a coherent, coordinated framework that guarantees citizens' rights while shielding society from the harms of the internet.[98] It provides "…a comprehensive national framework that outlines specific responsibilities for public and online platforms, including establishing transparent procedures for addressing harmful content and imposing penalties for non-compliance."[99] The paper also emphasises the need for collaborative efforts to ensure a safe digital environment for all categories of individuals including children.[100]

The Nigeria Data Protection Act, 2023 provides a framework for the protection of personal data.[101] It aims to ensure that data collectors and controllers deal with individuals' data within the prescribed principles while ensuring protection of their data rights. Section 31 specifically requires the consent of parents or guardians where the data to be dealt with relates to children, save where such dealing is for the best interests of the child or for a lawful purpose.

95 *Child Rights Act, 2003, https://placng.org/lawsofnigeria/laws/C50.pdf*
96 *The Nigeria Data Protection Regulation 2019: Implementation Framework, 2020, https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf*
97 *Advocacy for Policy and Innovation (API) and the National Information Technology Development Agency (NITDA), "White Paper on the Framework for an Online Harms Protection Bill in Nigeria, 2024," https://nitda.gov.ng/wp-content/uploads/2024/12/Updated-OHP-WHITE-PAPER-copy-compressed.pdf*
98 *Ibid.*
99 *Ibid.*
100 *Ibid.,p.14.*
101 *The Nigeria Data Protection Act, 2023, https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf*

The Law, Privacy and Safety Challenges and Solutions

The rapid growth of digital platforms across Africa has brought significant benefits, but poses many data privacy risks and threats. There is a greater fear for the vulnerable populace, specifically children who are often unaware of the dangers posed by their online activities and the risks of being exploited in harmful ways. Children are especially vulnerable to privacy violations due to their limited understanding of online dangers and insufficient regulatory protections. Reports such as in South Africa[102] reveal frequent misuse of children's data for advertising, particularly in food, educational apps and online platforms used during the COVID-19 pandemic, often without adequate parental consent. Moreover, parents have been cited in excessive sharing of their children's information that compromises their online safety and privacy rights.[103] Free sharing of information by parents and the laws which are poorly enforced have put children's online privacy at risk, particularly as social media and educational tools become more accessible. The following are some of the key challenges children in Africa face regarding privacy and protection online:

102 *Lewis, D., Bhoola, S., & Mafofoi, L. (2020). Corporate Fast-Food Advertising Targeting Children in South Africa. South African Child Gauge 2020, 62, https://ci.uct.ac.za/sites/default/files/content_migration/health_uct_ac_za/533/files/CG2020_ch3_corporate%2520fast-food%2520advertising%2520targeting%2520children.pdf*

103 *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.*

Cyberbullying and Harassment

The digital era has created a borderless world that has generated a new covert psychological form of bullying conveyed through electronic mediums. Cyberbullying takes various forms and tactics to target victims including sending inappropriate and often threatening and or abusive messages, disclosing embarrassing photos, and videos and spreading rumours, all of which form part of harassment, stalking and intimidation which aim to undermine the victim's self-esteem.[104]

Cyberbullying is a growing issue across Africa, fuelled by increasing internet penetration and widespread use of social media platforms. A UNICEF study in 2019 reported that approximately 34% of students had experienced some form of cyberbullying.[105] The Centre for Justice and Crime Prevention (CJCP)'s 2012 research on cyberbullying in South Africa notes several key factors behind the high prevalence of cyberbullying in South Africa.[106]

34%

of students had experienced some form of cyberbullying

The first is the widespread use of social media that has created a sense of anonymity online which creates a breeding ground for cyberbullying. The second is that because cyberbullying in most cases doesn't involve the physical aspect of abuse when compared to traditional forms of bullying, perpetrators often underestimate the effects it has on victims. Without education and awareness, it is difficult to comprehend the trauma and abuse that victims of cyberbullying face. Some of the reasons for cyberbullying include lack of awareness of the impact on victims, as well as boredom, jealousy and peer pressure which prompts perpetrators to bully others. Researchers have found that these reasons for cyberbullying are similar across other regions and are tied to specific risk factors including low self-esteem, social isolation, and mental health issues on the part of the victim.[107] Children targeted by cyberbullying often face long-term emotional and psychological issues, including anxiety, depression, low self-esteem, and post-traumatic stress disorder (PTSD).[108]

Another study conducted by Hinduja and Patchin has observed that victims of cyberbullying were twice as likely to attempt suicide when compared to youth who had never experienced cyberbullying.[109] Similar sentiments have been re-laid in their recent 2023 publication. [110]

104 *Peebles, E. (2014). Cyberbullying: Hiding behind the screen. Paediatrics & child health, 19(10), 527-528, https://pmc.ncbi.nlm.nih.gov/articles/PMC4276384/*

105 *Akbar Junior, "UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying" UNICEF, 03 September 2019, https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying*

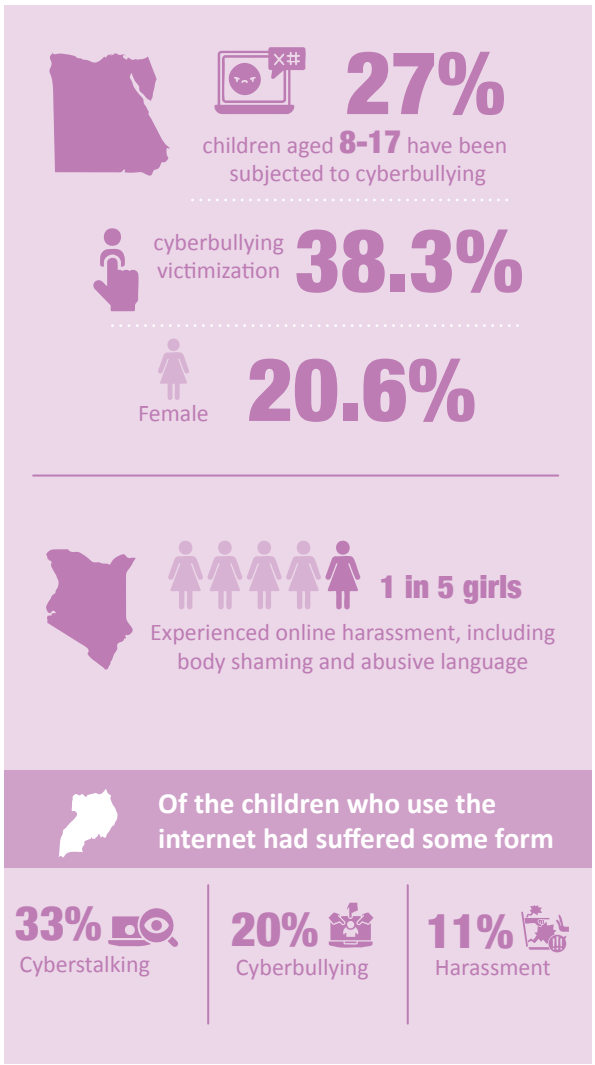
106 *Popovac, M., & Leoschut, L. (2012). Cyber bullying in South Africa: Impact and responses. Centre for justice and crime prevention, 13(6), 1-16, https://www.researchgate.net/publication/259117407_Cyber_bullying_in_South_Africa_Impact_and_Responses*

107 *Popovac, M., & Leoschut, L. (2012). Cyber bullying in South Africa: Impact and responses. Centre for justice and crime prevention, 13(6), 1-16, https://www.researchgate.net/profile/Masa-Popovac/publication/259117407_Cyber_bullying_in_South_Africa_Impact_and_Responses/links/0c96052a042a0e0c60000000/Cyber-bullying-in-South-Africa-Impact-and-Responses.pdf*

108 *Peebles, E. (2014). Cyberbullying: Hiding behind the screen. Paediatrics & child health, 19(10), 527-528., supra.*

109 *Ntsaluba, N. (2017). The cyber security legislative and policy framework in South Africa (Master's thesis, University of Pretoria (South Africa)), supra.*

110 *Peprah, P., Oduro, M. S., Okwei, R., Adu, C., Asiamah-Asare, B. Y., & Agyemang-Duah, W. (2023). Cyberbullying victimization and suicidal ideation among in-school adolescents in three countries: implications for prevention and intervention. BMC psychiatry, 23(1), 944, https://link.springer.com/content/pdf/10.1186/s12888-023-05268-9.pdf*



A survey by Crosstab in Egypt reported that 27% of children aged 8-17 have been subjected to cyberbullying. Further studies have reported that the prevalence of cyberbullying victimization was 38.3%, with 20.6% having been exposed to two or three forms while 4.1% were exposed to four or more forms of cyberbullying.[111] Female students, those under 18 years old, those with lower educational achievement, and those with higher daily internet use were more likely to experience cyberbullying. Cyberbullied students reported significantly higher levels of perceived stress and poorer mental well-being compared to non-cyberbullied students. Thus, the survey stated that cyberbullying is a significant problem among high school students in Egypt, with detrimental effects on their stress levels and mental well-being.[112]

Similarly, in Kenya, a report by Plan International in 2020 highlighted that almost 1 in 5 girls had experienced online harassment, including body shaming and abusive language.[113] In Uganda, a 2023 report reported that at least 33% of the children who use the internet had suffered some form of cyberstalking, 20% suffered cyberbullying and 11% suffered harassment.[114]

As evidenced with different countries there is an increase in cyberbullying of children especially those in schools. It is vital to call upon states to take targeted interventions and prevention strategies to address cyberbullying and promote the well-being of children in the digital age. Although prone to challenges, the digital era has brought new developments that have significant impact on their livelihood such as access to information, increase of knowledge and mode of socialization.

111 *Mohamed Wahba, N., Gomaa Ahmed, S., Mohammed Abdel-kader, S., & Gaber Hamza, H. (2019). Effect of a Cyber-Bullying Prevention Program. Egyptian Journal of Health Care, 10(3), 448-466, https://journals.ekb.eg/article_206583_9dffab20b7224e0dd4c725bf8ed27309.pdf*

112 *Ramadan, O. M. E., Alruwaili, M. M., Alruwaili, A. N., Elsharkawy, N. B., Abdelaziz, E. M., El Badawy Ezzat, R. E. S., & El-Nasr, E. M. S. (2024). Digital dilemma of cyberbullying victimization among high school students: Prevalence, risk factors, and associations with stress and mental well-being. Children, 11(6), 634.*

113 *Plan International, "Free to Be Online: Girls and Yound Women's Experiences of Online Harassment, 2020?" https://plan-international.org/uploads/2023/06/SOTWGR2020-CommsReport-edition2023-EN.pdf*

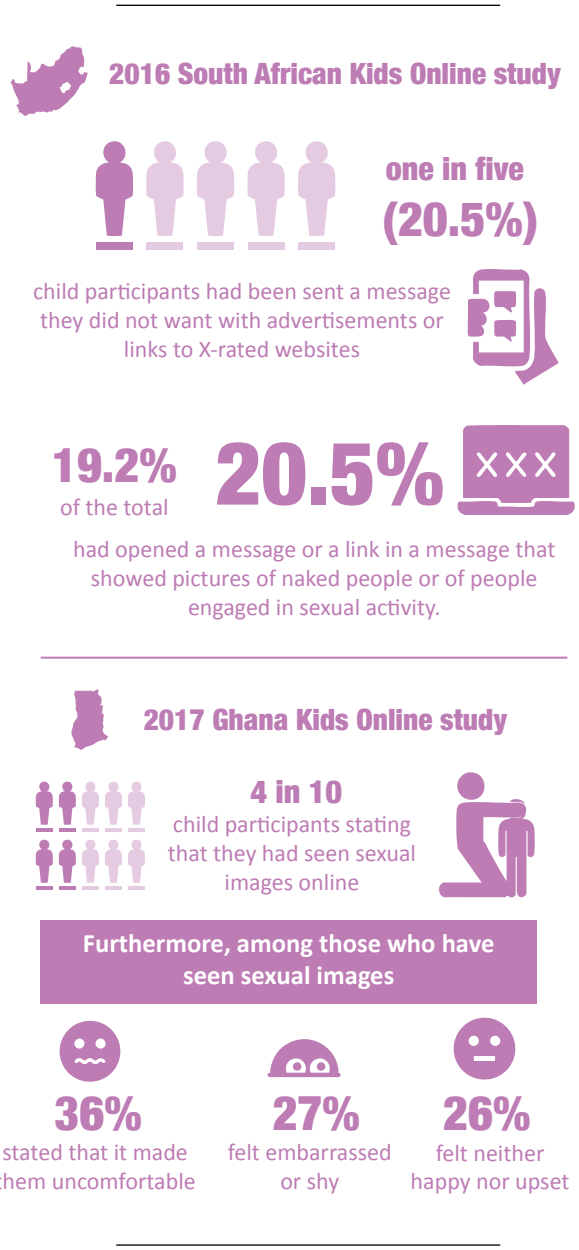
114 *Lydia Felly Akullu, "Silent Suffering: Cyberbullying among Celebrities' Children," The Monitor, 20 December 2023, https://www.monitor.co.ug/uganda/news/national/silent-suffering-cyberbullying-among-celebrities-children-4469932*

Exposure to Inappropriate Content

The unregulated nature of the internet in many African countries has led to children's increased exposure to harmful content, including violent and sexually explicit material. In Kenya, the Communications Authority has over the past years expressed concerns over access to inappropriate content often through social media platforms or gaming websites.[115] Nigeria has seen similar issues, where children access websites containing harmful material due to inadequate parental controls and weak regulatory frameworks. The Nigerian Communications Commission (NCC) has also highlighted the need for stronger internet safety regulations to shield children from such content.[116]

The 2016 South African Kids Online study, related to children's online practice found that in South Africa, one in five (20.5%) child participants had been sent a message they did not want with advertisements or links to X-rated websites. Furthermore, 19.2% of the total 20.5%, had opened a message or a link in a message that showed pictures of naked people or of people engaged in sexual activity.[117]

The findings of a similar study done in Ghana in 2017 mirrored those obtained from the South African study, with 4 in 10 child participants stating that they had seen sexual images online.[118] Furthermore, among those who have seen sexual images, 36% stated that it made them uncomfortable, 27% felt embarrassed or shy and 26% felt neither happy nor upset.[119] Additionally, there have been reports of similar concerns in Cameroon, Ethiopia, South Sudan, Uganda, Zambia where children to inappropriate content including pornography and sexualised images, sexual exploitation.[120]



115 *Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse, https://safeonline.global/wp-content/uploads/2023/12/DH-Kenya-Report_Revised30Nov2022.pdf .*

116 *NCC Gives Safety Tips on Child Online Protection (IV), https://www.businessremarks.com.ng/ncc-gives-safety-tips-on-child-online-protection-iv/*

117 *South African Kids Online: Barriers, opportunities & risk, A glimpse into South African children's internet use and online activities, http://globalkidsonline.net/wp-content/uploads/2016/06/GKO_Country-Report_South-Africa_CJCP_upload.pdf*

118 *UNICEF, G. (2017). Risks and opportunities related to children's online practices: Ghana country report, https://www.unicef.org/ghana/media/1791/file/Risks%20and%20Opportunities%20-%20Child%20Online%20Protection.pdf*

119 *Ibid.*

120 *MTN, "MTN advances online child safety efforts with new research and initiatives," 10 December, 2024, https://www.mtn.com/mtn-advances-online-child-safety-efforts-with-new-research-and-initiatives/ ; See also, ChildFund International and African Child Policy Forum, "Online exploitation and abuse of children in Africa on the rise," 30 May, 2024 https://childfundalliance.org/2024/05/30/online-exploitation-and-abuse-of-children-in-africa-on-the-rise/ ; and End Violence Against Children and UNICEF, "Online Risk And Harm For Children In Eastern And Southern Africa," https://safeonline.global/wp-content/uploads/2024/12/Online-Risks-Harm-Children-ESA-2023.pdf; ECPAT International, "Understanding African Children's Use of Information and Communication Technologies (ICTs): A Youth-Led Survey to Prevent Sexual Exploitation Online," https://ecpat.org/wp-content/uploads/2021/05/ICT-Research-in-AFRICA.pdf*

Online Predation and Exploitation

The increased internet penetration on the African continent has increased cases of exploitation and sex predation of children despite the potential benefits of increased access and use of ICTs. Reports indicate Kenya, Mozambique, South Africa, and Uganda have experienced an increase in online predation, including sexual exploitation and grooming.[121] The use of online platforms like Facebook and WhatsApp have overly exposed children to online grooming and exploitation with minimal supervision have aggravated the problem. Children have been exposed to requests for sexual contact made online and also gone ahead to physically meet the contacts.[122] The Internet Watch Foundation (IWF) reported that over 400 cases of child sexual abuse material (CSAM) involving Kenyan children had been flagged in 2021, with predators using social media platforms to lure vulnerable children.[123]

The United Nations Office on Drugs and Crime (UNODC) has identified and recognised the problem of sexual exploitation in West African countries especially in Ghana and Senegal. In response to the problem, it went ahead to launch a campaign that aims to combat the growing sexual exploitation.[124] The campaign among others focusses on awareness raising, encouraging reporting, promoting safe online practices, and advocating for legal action to end child exploitation of children.[125] These trends reflect a broader problem across the continent, where children remain at significant risk of online exploitation due to the lack of knowledge and awareness, sufficient legal protections and online safety measures.

Data Privacy Breaches

Children's personal data is increasingly being exploited by companies for commercial purposes, often without obtaining proper consent. The data protection laws in most of the 36 countries require parental consent before dealing with data relating to children by data collectors and controllers. For instance, Ghana, Uganda, South Africa, Botswana, Tanzania, Kenya and Rwanda laws on data are specific on protecting children's data. However, the actual enforcement of the laws is still lacking, particularly for online services targeting children. A report by the South African Human Rights Commission (SAHRC) in 2023 found several instances where children's personal data had been released to third-parties without parental consent.[126] In Egypt, there was exposure of sensitive data including names, addresses, dates of birth, and profile photos of tens of thousands of children which put their privacy at stake.[127] In Nigeria, many companies still fail to comply with data protection requirements regarding children, leading to breaches where children's data is collected and shared without adequate protection.[128]

These data breaches are becoming increasingly common across Africa since the laws are quite weak and do not offer robust protection. Private tech companies in these countries have also been put on the spot to meet their roles in ensuring child privacy and safety online and combat potentially illegal practices and violations and called upon to take appropriate measures to guarantee child privacy and safety.[129]

121 *ChildFund International and African Child Policy Forum, "Online exploitation and abuse of children in Africa on the rise," supra.*

122 *Ibid.*

123 *UNICEF. (2021). Ending Online Child Sexual Exploitation and Abuse. Lessons Learned and Promising Practices in Low and Middle Income Countries. Disponibil la https://www.unicef. org/documents/ending-online-child-sexual-exploitation-and-abuse. Accesat la, 10, 2024.*

124 *United Nations, "UNODC launches the 'Safer Children Online' campaign to combat online child sexual exploitation and abuse in Ghana and Senegal," https://www.unodc.org/westandcentralafrica/en/westandcentralafrica/stories/2023/safer-children-online-launch-en.html*

125 *Ibid.*

126 *Michalsons, "Department of Basic Education enforcement action | Consent," https://www.michalsons.com/blog/department-of-basic-education-dbe-enforcement-action-consent/76394#:~:text=Previously%2C%20the%20regulator%20found%20that,the%20department%20could%20not%20lawfully*

127 *Human Rights Watch, "Egypt: Data of Tens of Thousands of Students Compromised," 19 April, 2023, https://www.hrw.org/news/2023/04/19/egypt-data-tens-thousands-students-compromised*

128 *Iyoha-Osagie, T., & George, O. I. (2019). THE RIGHT TO ONLINE DATA PROTECTION OF CHILDREN: EXAMINING THE ADEQUACY OF THE LEGAL FRAMEWORKS TO COMBAT CHILD ONLINE DATA BREACHES IN NIGERIA. ABUAD Private and Business Law Journal, 3(1), 82-109.*

129 *Child Online Africa, 'Child Online Africa Calls for Stronger Regulations to Safeguard Children's Rights at Celebrity-Organized Events' (15 January 2025) https://www.childonlineafrica.org/press-releases/child-online-africa-calls-for-stronger-regulations-to-safeguard-children-s-rights-at-celebrity-organized-events/54 accessed 17 June 2025*

Inadequate Digital Literacy

Digital literacy is essential for children to understand online risks and protect their privacy, but many African countries face significant gaps in digital education. Shortfalls in digital literacy account for unintentional sharing of personal information, vulnerability to online risks such as phishing scams and general exposure to online digital security risks. Africa especially in the Sub-Saharan region is synonymous with this challenge which also stretches into slow or poor digital transformation.[130]

In Ghana, it is reported that a significant portion of students in public schools have received little to no formal digital literacy training.[131] This lack of awareness leaves children vulnerable to online risks such as identity theft and exploitation, as they often do not understand the implications of sharing personal information online. The issue is prevalent across many parts of Africa, including Botswana, Ghana, Kenya, Rwanda, Uganda, Zambia and Zimbabwe among others, particularly in rural areas, where access to digital education remains limited.[132] Similar trends are observed in countries like Nigeria where children are increasingly navigating the online space without the necessary tools to protect their privacy.[133]

Wide Penetration of Social Media without Adequate Safeguards

Social media platforms like Meta (Facebook), Instagram, WhatsApp, X (Twitter), SnapChat, YouTube and TikTok are popular among children across Africa. The use of these platforms entails the voluntary provision of personal information and information regarding friends and acquaintances but they pose significant risks to privacy.[134] Some have default public settings which leads to exposure of children to a wider audience such as social media influencers and increases the risk and chances of data breaches and misuse of information.[135] On the other hand, parents such as in Kenya, Ghana and South Africa, have been cited to be responsible for sharing excessive information about their children on various social media platforms while advertising companies are fond of consistent data breaches for targeted advertising.[136] Additionally, the level of protection is quite inconsistent and may be categorised as weak for Africa. In South Africa for instance, the information regulator of South Africa has on several occasions flagged several cases of data misuse by social media platforms that collect children's personal information without proper consent.[137] In Ghana, there have been several concerns over the use of children's data at celebrity events which though seamlessly harmless, put children's privacy, safety and well being at stake.[138] In Nigeria, a 2021 study by Paradigm Initiative found that social media companies were failing to comply with local data protection regulations, leaving children's information exposed to potential misuse.[139] These privacy violations are common across the continent, where the enforcement of data protection on social media platforms remains weak.

130 *Mhlanga, D., & Ndhlovu, E. (2024). Digital transformation in higher education and postgraduate research supervision in Africa: A critique of 4ir-based interventions in open distance education. Xue bao (Xi nan jiao tong da xue, China), 59(5).*

131 *Asare-Yeboah K and others, 'Status of implementation of the ICT Curriculum in Ghanaian Basic Schools' (2014) 3 (8) Journal of Arts and Humanities 48*

132 *Victoria Kwakwa, "Empowering Africa's youth: Bridging the digital skills gap," Nasikiliza, 25 July, 2024, https://blogs.worldbank.org/en/nasikiliza/empowering-africa-s-youth--bridging-the-digital-skills-afe-gap*

133 *UNICEF, "Protecting Children in the Digital World: A Guide for Parents and Teachers," https://www.unicef.org/nigeria/protecting-children-digital-world*

134 *Media Monitoring Africa, "South African Children Demand Better Online Privacy Protections - Media Monitoring Africa," 20 November 20124, https://www.mediamonitoringafrica.org/south-african-children-demand-better-online-privacy-protections/*

135 *S Goliath 'The Protection of Personal Information Act 4 of 2013: Child social media influencers and their right to privacy' (2024) 1 African Journal on Privacy & Data Protection 81-98 https://doi.org/10.29053/ajpdp.v1i1.0005*

136 *Lewis, D., Bhoola, S., & Mafofoi, L. (2020). Corporate Fast-Food Advertising Targeting Children in South Africa. South African Child Gauge 2020, 62, https://ci.uct.ac.za/sites/default/files/content_migration/health_uct_ac_za/533/files/CG2020_ch3_corporate%2520fast-food%2520advertising%2520targeting%2520children.pdf*
Lewis, D., Bhoola, S., & Mafofoi, L. (2020). Corporate Fast-Food Advertising Targeting Children in South Africa. South African Child Gauge 2020, 62, https://ci.uct.ac.za/sites/default/files/content_migration/health_uct_ac_za/533/files/CG2020_ch3_corporate%2520fast-food%2520advertising%2520targeting%2520children.pdf
Lewis, D., Bhoola, S., & Mafofoi, L. (2020). Corporate Fast-Food Advertising Targeting Children in South Africa, Supra.

137 *Simnikiwe Mzekandaba, "South African youth in dark about data protection law," IT Web, 29 January, 2025, https://www.itweb.co.za/article/south-african-youth-in-dark-about-data-protection-law/O2rQGMAE46rMd1ea*

138 *Child Online Africa, "Child Online Africa Calls for Stronger Regulations to Safeguard Children's Rights at Celebrity-Organized Events," https://www.childonlineafrica.org/press-releases/child-online-africa-calls-for-stronger-regulations-to-safeguard-children-s-rights-at-celebrity-organized-events/54*

139 *Paradigm Initiative, "Digital Rights and Inclusion in Africa, 2021," https://paradigmhq.org/wp-content/uploads/2022/05/Londa-English-Report-real.pdf ; Paradigm Initiative, "Digital Rights and Inclusion in Africa, 2020," https://paradigmhq.org/wp-content/uploads/2021/05/Londa-Digital-Rights-and-Inclusion-in-Africa-Report-2020-lr.pdf*

Economic and Geopolitical Challenges

The digital divide and lack of infrastructure in rural areas exacerbate privacy risks for children in Africa. Across the region and in the study countries, children in rural regions have little to no access to digital literacy programs or secure internet connections, making them more vulnerable to privacy violations.[140] The regions are also characterised by limited access to technology and weak governance structures that make it difficult for the government to enforce privacy regulations effectively.[141]

The economic constraints in many African countries also mean that governments often lack the resources to implement comprehensive child protection policies. This is further compounded by political instability in countries like Mali and Ethiopia, and West Africa where conflict has further disrupted the development of cybersecurity infrastructure. The economic and geopolitical challenges are widespread across Africa, contributing to the increased privacy risks faced by children as opposed to the desired and enhanced child protections online.[142]

Limited Focus on Children in Existing Legal Frameworks

While the ACRWC, along with the UNCRC, emphasize the need to protect children's privacy, few national laws specifically address children's online privacy in detail. Most African countries including Algeria, Botswana, Egypt, Ghana, Kenya, Nigeria, Rwanda, Southern Africa, Tanzania, and Uganda treat privacy laws as general provisions, without considering the unique vulnerabilities faced by children in the digital environment. Most of the laws lack explicit provisions for children's privacy, making it difficult to enforce protections tailored to their specific needs in the online space.

For example, the above-mentioned countries demonstrate this shortfall, despite Africa being the first region in the world to implement a child online safety and empowerment policy.[143] For instance, Uganda's Computer Misuse Act and Tanzania's Cybercrimes law focuses more on cybercrime than on protecting individuals, especially children, from data breaches or misuse. Similarly, Cameroon does not have a child-specific focus in its digital or privacy laws, leading to a lack of comprehensive protection for children navigating online spaces.[144] Further still, while South Africa and Kenya have made significant progress in developing relevant laws compared to other states, gaps still exist.

140 *Ibid.*

141 *Ibid.*

142 *Moestue, H., & Muggah, R. Digitally Enhanced Child Protection, https://igarape.org.br/wp-content/uploads/2014/11/Artigo-estrategico-10-Child-Protection-4.pdf; Keeley, B., & Little, C. (2017). The State of the Worlds Children 2017: Children in a Digital World. UNICEF. 3 United Nations Plaza, New York, NY 10017, https://files.eric.ed.gov/fulltext/ED590013.pdf*

143 *African Union, "Africa Has Become The First Region in The World to Implement a Child Online Safety and Empowerment Policy," 23 May, 2024, https://au.int/en/pressreleases/20240523/child-online-safety-and-empowerment-policy-africa-union*

144 *Ibid.*

Weak Enforcement and Institutional Capacity

In many African nations, even where laws exist, enforcement remains a major challenge. Regulatory bodies tasked with protecting children's privacy online are often under-resourced and lack the necessary capacity to monitor and enforce compliance. For example, in Kenya, while the Data Protection Act includes provisions that could protect children's online privacy, the Data Commissioner's Office is underfunded and understaffed, which limits its ability to enforce these provisions, particularly in rural areas where digital literacy is low.[145] Similarly, Uganda's Data Protection Office suffers from under staffing and under financing which further limits its operations and efficiency. In Nigeria, many companies particularly those offering online services as noted earlier are not aware of the various legal obligations. In Zambia, ineffective law enforcement has weakened child protection against pornography and sexual exploitation.[146] Similarly, in Zambia, the existing reporting mechanisms for online violations are inadequate making it difficult to track online crime against children.[147]

The inadequacy in compliance is problematic for children's privacy, as online platforms continue to collect data without proper oversight or the consent of guardians. Across the study countries, there is a glaring lack of the relevant infrastructure and human resources to oversee and regulate the digital space effectively, leaving children at risk of online exploitation and data breaches. Additionally, the weak enforcement of laws and reports of online crime against children such as sexual exploitation has exacerbated the problem.[148]

Limited Public Awareness

A significant gap in institutional protection across African countries including in Algeria, Botswana, Egypt, Ghana, Nigeria,[149] South Africa, Burundi, DRC, Kenya, Tanzania, and Uganda lack public awareness and digital literacy, which makes it harder to implement and enforce privacy regulations.[150] While laws exist to protect personal data, many parents, guardians, and children themselves are unaware of their rights and the risks posed by online data collection. This lack of awareness allows for widespread non-compliance with privacy laws, as children and their families are not equipped to challenge violations or understand how to protect their personal information online.

Without widespread education on privacy and data protection, children are particularly vulnerable to exploitation in the digital space. Governments in these countries are yet to prioritize digital literacy programs, leaving a critical gap in ensuring the legal protections for children are practically effective. The situation is particularly worse in rural areas, where children often access the internet without any form of supervision, making them more vulnerable to inappropriate content. This exposure as earlier noted can cause psychological distress and lead to behavioural changes, a challenge that is becoming increasingly common across African countries with rising internet penetration.[151]

145 *Advocacy Brief: Enhancing Policy Responses to Addressing Child Sexual Exploitation and Abuse (CSEA) in Kenya (January 2023) – ReliefWeb, https://reliefweb.int/report/kenya/advocacy-brief-enhancing-policy-responses-addressing-child-sexual-exploitation-and-abuse-csea-kenya-january-2023*

146 *Goitom, Hanibal, "Zambia: Ineffective Law Enforcement Weakens Child Protection Enforcement," https://www.loc.gov/item/global-legal-monitor/2008-07-02/zambia-ineffective-law-enforcement-weakens-child-protection-enforcement/*

147 *Policy Brief: Protecting Children's Rights in the Digital Environment, https://www.wvi.org/sites/default/files/2023-06/Policy%20Brief%20on%20Children%27s%20Rights%20in%20the%20Digital%20Environment_0.pdf*

148 *Africa Fast Becoming The Global Hotspot For Child Sex Tourism And Online Sexual Exploitation - Graça Machel Trust: https://gracamacheltrust.org/2019/11/27/africa-fast-becoming-the-global-hotpot-for-child-sex-tourism-and-online-sexual-exploitation/*

149 *Children's online safety in Nigeria: the government's critical role - LSE Blogs: https://blogs.lse.ac.uk/parenting4digitalfuture/2018/09/12/childrens-online-safety-in-nigeria/ ; UNICEF, "Protecting Children in the Digital World: A Guide for Parents and Teachers," supra.*

150 *EA struggles to protect children online as digital life quality stagnates - The EastAfrican: https://www.theeastafrican.co.ke/tea/sustainability/ea-struggles-to-protect-children-online-4528070*

151 *Day Of The African Child 2023 Theme: The Rights Of The Child In The Digital Environment Concept Note - ACERWC: https://www.acerwc.africa/sites/default/files/2023-02/DAC%20CONCEPT%20NOTE%202023_EN.pdf*

Slow Adoption and Compliance with International Standards

While many African nations have signed international treaties such as the UNCRC and the ACRWC, the domestication and enforcement of these standards remains slow because, in some countries, there is a dualist legal system that applies treaties only after domesticating legislation has been adopted. This has left children on the continent in a vulnerable state. Factors contributing to this challenge include resource constraints for funding, training and enforcement, lack of prioritisation by governments and the differences in culture and the laws.

In countries like Burundi, Kenya, Rwanda, Tanzania and Uganda, poor digital infrastructure, inadequate awareness, and the inadequacy of laws and policies on standards of child protection online and laxity and reluctance of families have contributed to the problem.[152]

Similarly, while international frameworks are recognized, the process of aligning national laws with these frameworks is delayed. This gap creates legal inconsistencies, where international standards exist on paper but are not translated into national laws or institutional practices, leaving children's privacy rights inadequately protected in the online sphere. In countries that have incorporated elements of international agreements, such as South Africa and Kenya, full compliance with international privacy standards, such as the GDPR or other child-specific protections, remains incomplete. This slow adoption hampers efforts to create safe online environments for children and exposes them to ongoing risks.

152 Vincent Owino, "EA struggles to protect children online as digital life quality stagnates" The EastAfrican 17 February 2024, https://www.theeastafrican.co.ke/tea/sustainability/ea-struggles-to-protect-children-online-4528070

Conclusion

The digital landscape presents both remarkable opportunities and significant threats to child privacy in Africa. With children increasingly active online, they are particularly vulnerable to a range of risks, from data breaches and exploitation to invasive data collection and profiling. This report has underscored the common issues, emerging challenges and the practices in child protection online. It has highlighted the thin approach of states to comprehensively address child protection issues online despite their recognition of children's online. Hence, stakeholders across the region should engage in a collective manner to promote awareness on the dangers resulting from pervasive online access to child privacy and push for safeguards and greater protection for children's rights online across African states. Overall, several data protection frameworks referenced in this report fall short of the specific and robust safeguards for children, and exclude a number of principles such as accountability and transparency, lawfulness, fairness, and transparency, limitation and purpose set out under international law. Indeed, only Kenya, Nigeria, and South Africa are considered to have laws that are relatively robust.[153] Going forward, there needs to be robust and meaningful accountability from all stakeholders and more importantly, a shift from mere rhetoric to strategic action. The policy environment should be strengthened by establishing corresponding institutional mechanisms that are well-equipped to provide oversight and are facilitated to learn best practices from other jurisdictions through international cooperation.

153 *See for instance, Valentine, J. A. (2023). Governance and the Digital Economy in Africa Technical Background Paper Series-Vulnerabilities of ICT Procurement, https://documents1.worldbank.org/curated/en/099051924164028010/pdf/P1724171504d3f03e19f251b7aa4316bb23.pdf*

Recommendations

This study has analysed the developments and trends in child protection online in Africa. The status, existing legal frameworks and practices reveal the need for a multifaceted approach that can improve the protection of children online. The key stakeholders in this discourse include governments, civil society organisations, technology sector, media and academia among others. These players must take steps that facilitate and buttress the protection of children online while promoting their digital rights. Below are some of the emerging recommendations which the various stakeholders should undertake to the effect.

Governments

- The Parliaments should develop and enact specific national frameworks that focus on protecting children's privacy and protection in digital spaces, with clearly defined protections tailored to children's unique needs and vulnerabilities.
- Swiftly ratify and domesticate international and regional frameworks such as the Malabo Convention, which provides legal obligations on states and a framework for cyber security and personal data protection including for children. The domesticated laws should align with the regional international standards like the UN Convention on the Rights of the Child (UNCRC) and the African Charter on the Rights and Welfare of the Child.
- Finance, develop and implement national strategies that primarily target government agencies including the judiciary, data protection authorities and law enforcement actors, educators, parents, and the private sector and set out their roles and responsibilities in protecting children online.
- Promote digital literacy and awareness raising by integrating them in school curricula and public awareness programmes on media like television, radio and social media that target parents and caregivers of guardians.

Civil Society Organisations

- Advocate for the enactment of laws that target and address online violence against children including cyberbullying, cyber harassment, sexual exploitation and child pornography. Where there are existing frameworks but with gaps, CSOs should advocate for amendment to make them more intentional and progressive on countering online violence against children.
- Raise awareness through education, capacity building and media campaigns including social media, television and radio on the dangers of child exploitation and abuse and ways to end them.
- Collaboratively provide direct support and intervention measures for the victims of online crimes against children such as through offering counselling and establishing safe reporting mechanisms and helplines for rapid response to emerging risks and perpetrations.
- Conduct evidence-based research that highlights the main online risks facing children, the prevalent rates and share the findings with other stakeholders including regional and international organisations, academia and media among others.

International Organisations and Development Partners

- Collaboratively work on a multi-pronged strategy that encompasses strengthening of legal and policy frameworks, enhances capacity building and awareness raising and strengthens public-private partnerships so as to mitigate common online threats and risks to children.

Technology Sector

- Design and implement child-friendly products and services that incorporate robust data protection measures, minimise data collection and retention regarding children and install clear child age verification and parental controls to restrict children's access to restricted content.
- Work hand in hand with other stakeholders including CSOs, governments, academia, media and other players in initiatives that seek to address online child abuse like in trainings, research and technical support developing and implementation of digital literacy and online safety programmes.
- Ensure accountability and transparency by publishing transparency reports on their efforts to protect children online, provide information on content moderation practices, reporting and collaboration and conduct independent audits of the online measures that seek to ensure accountability.

Media

- Report objectively and ethically, all cases involving exploitation of children and the publication of false information, disinformation, graphic images or details that potentially interfere with child privacy, traumatise or spread harmful content against children.
- Collaboratively with other players including governments, CSOs, tech companies, raise awareness on the risks of online child abuse and how to identify and report such cases. This can be done through educational and literacy programmes.
- Continually monitor, document and report all incidences of child harmful content to the relevant authorities to ensure transparency and accountability.
- Engage in responsible advertising and work with advertisers to avoid deception and the popularization of products and practice which are harmful to children.

Academia

- Conduct evidence based inter-disciplinary research which delves into the multifaceted nature of issues that affect child protection and rights online including cyberbullying, cyber harassment, sexual exploitation and grooming, and the social and psychological impacts they have on them.
- Develop and design specialized programmes on child rights and protection in the online spaces and integrate them in the school curricula.
- Collaborate with other stakeholders including governments, CSOs, tech companies in research and development of tools that promote and address child safety online.

Parents and the General Community

- Foster open and honest conversations with children about their online activities to ensure safe interaction with the online spaces. This could expand into awareness raising activities to teach children about online safety and protection.
- Supervise children's online activities and apply parental control tools to monitor and filter content as a safe measure strategy.
- Collectively challenge social and cultural norms which condone online harms against children and promote a culture of respect and responsibility.

This publication has been made possible with financial support from Norway through the International Center for Not-for-Profit Law (ICNL). The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the Government of Norway.