African Journal on Privacy & Data Protection

To cite: EC Joseph & ME Mwakisiki 'Protection of children's rights to privacy in cyberspace: A bird's eye view over the Tanzanian legal framework ' (2025) 2
African Journal on Privacy & Data Protection 98-125

Protection of children's rights to privacy in cyberspace: A bird's eye view over the Tanzanian legal framework

*Elias C Joseph**
Assistant lecturer, Moshi Cooperative University; practising advocate, Kilimanjaro, Tanzania

*Mwakisiki E Mwakisiki***
Practising advocate, Kilimanjaro, Tanzania

Abstract

Children's privacy rights in cyberspace are essential aspects of today's digital age. This is because children's exposure to cyberspace is inevitable given its relevance in children's communication, education, recreation opportunities and cultural exchange. Moreover, these rights underpin other important rights, namely, dignity, public participation, information access, freedom of expression and right to associate. The right becomes more pressing given an increase in children's connectivity in cyberspace. This article focuses on unveiling the inevitable ever-growing landscape of child exposure to cyberspace in Tanzania and the current and potential privacy risks associated with their navigation in cyberspace. The article also explores the legal and policy challenges, implications and efforts to address these challenges. The study employs doctrinal analysis, archival research and case

* LLB (Mzumbe University) PGDLP (Law School of Tanzania) LLM (University of Iringa); josephbr945@gmail.com
** LLB (Moshi Cooperative University) PGDLP (Law School of Tanzania); mwakisiki.mwakisiki@mocu.ac.tz

study methodologies. Appropriate human rights instruments of international nature were studied to situate the discussion to a broader perspective. Additionally, secondary materials such as government reports, surveys, reports from non-state actors and newspapers were used. The approach ensures a thorough analysis of the complex socio-legal issues surrounding children's privacy in cyberspace. The study further employs a comparative analysis and bench marking of the existing legal and policy framework against international best practices and standards. The purpose is to draw lessons from and to inform the suggested reforms in the law on minors' privacy in Tanzania. The article underscores that, for children to peacefully access and exploit opportunities brought by the virtual world, a comprehensive legal and policy framework tailored towards protecting children's rights in cyberspace becomes essential. Collective measures between actors are imperative in safeguarding children's privacy rights in cyberspace.

Key words: right to privacy; child privacy; cyberspace; Tanzanian legal framework

1 Introduction

The virtual world has become an integral part of every facet of human life, influencing the way in which people engage, connect and communicate.[1] In today's technologically astute society, children are increasingly immersed in the virtual world, making their involvement in the digital realm inevitable. Their engagement in the virtual world is seen as a necessary means for them to share and effectively engage in their civic life.[2] With over two billion children forming a significant portion of the global population,[3] more than 70 and 90 per cent of children had access to laptops and smartphones respectively.[4] This significant exposure to the virtual environment brings about both benefits and a spectrum of risks.[5] For instance, research indicates that more than 300 million children, experience online sexual exploitation and abuse yearly.[6] Therefore, while it is true that the virtual world offers numerous benefits to children's growth and development, it also renders them more vulnerable to privacy breaches and exploitation.[7]

1 According to art 1 of the Convention on the Rights of the Child, a child means every human being below the age of 18 years unless under the law applicable to the child; the majority is attained earlier.

2 I Milkaite & E Lievens 'Children's rights to privacy and data protection around the world: Challenges in the digital realm' (2019) 10 *European Journal of Law and Technology* 4.

3 Children in the World by Country 2024, https://worldpopulationreview.com/country-rankings/children-in-the-world-by-country (accessed 5 June 2024).

4 Share of children and adults worldwide using selected digital devices as of December 2023, https://www.statista.com/statistics/1483634/children-adult-devices-access-worldwide/ (accessed 13 December 2014)

5 M Cunha 'Child privacy in the age of web 2.0 and 3.0: Challenges and opportunities for policy' Innocenti Discussion Paper (2017) 6.

6 Scale of online harm to children revealed in global study, https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-global (accessed 13 December 2024).

7 UNICEF 'Children's online privacy and freedom of expression' Industry Tool Kit (2018) 4.

Fascinated by the virtual world and because of their immaturity, children may inadvertently share their data, putting themselves at risk of cyber-bullying and exposure to inappropriate content, among other dangers.[8] For these reasons, their security in online atmosphere has become an emerging topical and critical issue gaining prominence across jurisdictions.[9] Furthermore, the need to address children's privacy rights hinges on the reality that it is a fundamental right underpinning other essential rights including freedom of expression, information and association.[10] Thus, protecting children's privacy rights not only is an imperative human right but also a conditional precedent for building a stable and prosperous nation in the future.

As in the case of many African countries, Tanzania has fully embraced technological advancement, integrating it in different spheres of life, including children's education and development.[11] Over the past decade, Tanzania has experienced a demographic shift towards a youthful population, with approximately 43 per cent of its population comprising children below 15 years.[12] Although statistics on children's involvement in cyberspace in Tanzania are scant, the few available are worth mentioning. The 2022 report by ECPAT, INTERPOL and UNICEF shows that 67 per cent of minors of 12 to 17 years are internet users.[13] Such an ever-increasing number of children's population, coupled with their growing involvement in cyberspace, indicates the need for a critical examination of their rights while navigating these cyber platforms. This need is further underscored by the fact that children previously were not part of both international and domestic debates on technological regulation, which so far has resulted in the promulgation of regulations that do not specifically consider children's welfare.[14] Additionally, children are now at the centre of several global agendas such as the 2030 Global Agenda which, among others, aims at building a bright future and safer environment where children can harness their full potential and secure their rights.[15]

Appreciating the essence of protecting children's rights and upholding its international obligations, Tanzania has so far made significant strides in developing specific legal frameworks aiming at safeguarding children's rights. The enactment of the Child Act of 2009, the Cyber Crimes Act of 2015 and the

8 L Fourie 'Protecting children in the digital society' in J Grobbelaar & C Jones *Childhood vulnerabilities in South Africa: Some ethical perspectives* (2020) 232-234.

9 M Macenaite 'Protecting children's privacy online: A critical look to four European self-regulatory initiatives' (2016) 7 *European Journal of Law and Technology* 2.

10 Privacy International and Tanzania Human Rights Defenders Coalition *Stakeholder Report* (2015) 2.

11 K Okeleke '*Digital transformation in Tanzania: The role of mobile technology and impact on development goals'* (Groupe Speciale Mobile Association 2019) 19.

12 *'The 2022 Population and Housing Census: Age and Sex Distribution Report, Key Findings, Tanzania'* (2022) 9.

13 ECPAT, INTERPOL & UNICEF *Disrupting harm in Tanzania: Evidence on online child sexual exploitation and abuse* (Global Partnership to End Violence against Children 2022) 24.

14 Okeleke (n 11) 18.

15 Adopted by United Nations member states on 25 September 2023; all forms of child violence, abuse and exploitation were integrated as an international development agenda (para 16.2).

Personal Data Protection Act of 2022 supports this assertion.[16] Complementing these legislative initiatives, Tanzania recently launched the Child Online Protection (COP) campaign, which aims at safeguarding children in digital realms.[17] The Tanzania Communication Regulatory Authority, on its part, through the Computer Emergency Response Team (CERT), has regularly been issuing guidelines to parents and guardians on practices enhancing children's security while online.[18] Despite these efforts, more is still to be done, as the risks children face in the digital environment keep on increasing.[19] Against this backdrop, it thus is important to evaluate the Tanzanian legal framework, assessing the degree at which minor's privacy rights in the digital setting have been upheld and realised.

This article delves into the intricate landscape of the cyberspace by examining how some activities involving children have necessarily shifted their environment from physical to virtual environment. It unpacks the inevitability of cyberspace for children and the various risks and implications associated with their exposure to it. It explores the legal, institutional and other measures implemented to preserve children's privacy online both in Tanzania and globally. The article emphasises the importance of collaborative measures among relevant stakeholders, for instance, the government, regulators, technology companies, internet access providers, children, and parents or guardians, in an endeavour to create a safe online atmosphere for children.

The article is organised in six parts, starting with this introductory part, which provides a brief background and underscores the necessity of safeguarding children's privacy in cyberspace. The following part offers an elucidation of important concepts, namely, child protection, cyberspace and child privacy, while offering the divergent views between Afrocentric and Eurocentric schools on the conception of the term 'privacy'. The subsequent part provides an account of the trend of exposure of children in cyberspace and the prevalent violations of their privacy rights. The fourth part makes an evaluative analysis of existing legal frameworks at domestic, regional and international levels, and the ensuing part examines the position of the Tanzanian courts in vindicating children's privacy rights. The article concludes by encapsulating the main findings and recommendations derived from the preceding discourse.

16 *Stakeholder Report* (n 10) 4-7.
17 The campaign to protect children online launched on 19 February 2024, https://dailynews.co.tz/campaign-to-protect-children-online-launched/ (accessed 13 December 2024).
18 Protection of children online, https://www.tcra.go.tz/pages/child-online-protection-cop (accessed 13 December 2024).
19 Okeleke (n 11) 45.

2 The conceptions of 'child protection', 'cyberspace' and 'child privacy'

To develop a well-founded understanding of the gist of this work, it is significant to conceptualise the terms 'child protection', 'cyberspace' and 'child privacy' in the purview of this article. This is imperative because some concepts bear relative connotations depending on the scholarship taken as a standpoint, the societal characteristics, and the economic and cultural environment. Child protection entails safeguarding children against abuse, violence, neglect, exploitation together with implementing several efforts to respond to harm directed towards children.[20] The concept broadly includes protection in all settings, the cyber environment included.[21] Crucially, it encompasses all efforts for deterrence of and response to all types of children's ill-treatment.[22] Emphasising the protection of children's privacy, in *Centre for Child Law & Others v Media 24 Limited & Others*,[23] the South African Court held that centrality of children's privacy rights to their self-identity renders it even more crucial than for other demographic groups.

On the other hand, the term 'cyberspace', as defined in *Webster's new world telecom dictionary*,[24] refers to the virtual environment formed by interconnected computers and computer networks on the internet. It entails data, objects and activities that exist in the network itself.[25] Essentially, it represents the realm where computers and individuals engage, typically through the internet.[26] The term is synonymous with the term 'internet' and, therefore, anything happening on the internet is considered to take place within cyberspace rather than at the physical location of the servers or users.[27] Coming to the concept of 'child privacy', one of the difficulties facing effective protection of privacy rights is the rhetorical battle cry in a plethora of unrelated contexts of the notion of privacy.[28] Some claim that the notion encompasses a variety of interconnected yet distinct notions, including the right of being alone, controlled access to oneself, secrecy, power

20 AK Johnson & J Sloth-Nielsen 'Child protection, safeguarding and the role of the African Charter on the Rights and Welfare of the Child: Looking back and looking ahead' (2020) 20 *African Human Rights Law Journal* 644.
21 As above.
22 As above.
23 [2019] ZACC 46.
24 R Horak *Webster's new world telecom dictionary: A comprehensive reference for telecommunication technology* (2007).
25 Protecting Children in Cyberspace, https://mpra.ub.uni-muenchen.de/17150/ (accessed 5 June 2024).
26 SMH Collin *Dictionary of ICT* (2004).
27 Johnson & Sloth-Nielsen (n 20) 644.
28 *The right to privacy in the digital age in Africa: Module 1 – Introduction to privacy and data protection* Massive Open Online Course (MOOC) presented by the Centre for Human Rights, University of Pretoria, supported by Google, 27 May 2021.

over individual data, and personal hood.[29] However, a common thread among these diverse interpretations is the desire for control over personal information.[30]

Contextually, some African authors have been quick to point out that the African conception of the term 'privacy' relatively differs from the outside world. They assert that the prevailing understanding of privacy is Eurocentric and does not align with African realities.[31] Thus, to them, a proper definition of the term 'privacy' has to take on board the inherent features of communality, collectivism and interdependence existing in African societies.[32] Moreover, child privacy should be conceptualised taking on board the parental role of reasonable control over the behaviour of their children.[33] However, this school is still debatable given that, to date, there is no universally agreed upon definition of privacy in African social-political context.[34] Therefore, the notion of child privacy online can also be discussed in conjunction with the above viewpoint, because similar sentiments arise when discussing concepts relating to children's privacy in cyberspace. Child privacy in cyberspace consequently is associated with exposure to private data and various forms of harm, including solicitation of children for sexual purposes, exposure to inappropriate content, manipulation, surveillance, hacking and damage to reputation, among others.[35] According to the United Nations (UN), the phrase 'children's online privacy' encompasses all facets of child's privacy, including physical, communication, informational and decisional aspects.[36]

To this end, it is argued that the efforts by Afrocentric views to conceptualise privacy, taking on board the inherent characteristics in Africa, have not been realised. The article notes further that such a dilemma might have contributed to the information gap regarding the conception and essence of children's privacy online in African jurisdiction. In Tanzania, for instance, the Tanzania Communication Regulatory Authority (TCRA) issues quarterly statistical reports on the trend of accessibility and involvement of people in the internet. The report does not show the trend in terms of age and, therefore, one cannot comprehensively assess the growth of children's experience in the internet.[37] This situation is alarming given that any contemporary landscape on data protection should take on board the needs of the children. The World Health Organisation (WHO) emphasises that children's concerns need be at the core of

29 EC Joseph 'Right to privacy in mobile communication in Tanzania' (2022) 1 *Journal of Contemporary African Legal Studies* 48.
30 A Makulilo 'The quest for information privacy in Africa' (2018) Book Review Reply, *Journal of Information Policy* 317-337
31 As above.
32 Joseph (n 29) 48.
33 Art 10 African Charter on the Rights and Welfare of the Child, 1990.
34 J Neethling 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 19.
35 OM Sibanda 'Towards a more effective and coordinated response by the African Union on children's privacy online in Africa' (2022) *African Human Rights Yearbook* 158.
36 UNICEF (n 7) 4.
37 Tanzania Communications Regulatory Authority, Quarterly Statistics Reports, https://www.tcra.go.tz/ (accessed 26 December 2024).

any Sustainable Development Goals (SDGs).[38] It was imperative, therefore, for TCRA reports to have a section showing the trend of children's accessibility to the internet to inform the government on the potential and magnitude of their risks while navigating there.

3 Children's exposure to the cyberspace

Lifestyle changes brought about by the advancement of information and communication technology have not left children behind. Today's children grow with the internet, to the extent of becoming digital natives.[39] The internet and other online conduits have attracted children in their endeavour to engage, communicate and learn.[40] Millions of children access the internet annually for educational and recreational purposes.[41] However, in their attempt to explore the opportunities available over the internet, such as playing, learning, self-expressing, experimenting relationships and identities, they find themselves unwittingly sharing an increasing amount of their personal data to service providers.[42]

The ever-increasing children's involvement in the digital realm stems from, among other things, concerted efforts to achieve digital inclusion and the essence of bridge the existing digital divide.[43] In 2020, for example, it was estimated that 87 per cent of children in advanced economies and 6 per cent in emerging economies had internet accessibility.[44] Additionally, according to the global telecommunication authority, 65 per cent of young persons in the developing world connect to the internet for various activities.[45] Irrespective of the digital divide in Africa, by 2021 about 40 per cent of young people were able to get the internet connection in any of its forms.[46] A survey conducted in Ghana on minors' engagement in the digital realm has shown that, on average, children begin using the internet at the age of 12 years, with four out of ten children accessing the

38 Children as a Basis for Sustainable Development, https://sustainabledevelopment.un.org/content/documents/6449100-Children%20as%20a%20basis%20for%20sustainable%20development.pdf (accessed 26 December 2024).

39 OECD 'The protection of children online: Risks faced by children online and policies to protect them' (2011) *OECD Digital Economy Papers* 179.

40 A Singh & T Power 'Understanding the privacy rights of the African child in the digital era' (2021) 21 *African Human Rights Law Journal* 100.

41 M Medaris & C Girouard 'Protection of children in the cyberspace: The ICAC task force programme' (2002) *Juvenile Justice Bulletin* 1.

42 M Macenaite & E Kosta 'Consent for processing children's data in the EU: Following in US footsteps?'(2017) 26 *Information and Communications Technology Law* 146.

43 See item 4 of the introduction to General Comment 25 on children's rights in relation to the digital environment.

44 UNICEF & 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) 4.

45 Joining Forces Alliances 'Protecting children in the digital environment' (2023), cited from the 2022 Safer Internet Day – We must act together to put children and young people at the centre of our digital policies.

46 A Singh & T Power 'Understanding the privacy rights of the African child in the digital era' (2021) 21 *African Human Rights Law Journal* 100.

internet at least once a week.[47] This indicates that children frequently utilise the internet and they do so at a relatively young age. In Africa, generally, the survey shows that out of an estimated 590 million internet users as of May 2022, one-third were children.[48]

In Tanzania, while there has not been an extensive and regular survey on the trend of children's involvement in cyberspace, a few available reports are worth noting. The available data shows that internet penetration stands at 37.6 per cent with a growth rate of 20.024 per cent. In August 2023, the internet users in the country reached 23 142 100.[49] Furthermore, the statistics indicate that as of June 2022, approximately 67 per cent of young persons above 12 and below 18 years in Tanzania were internet subscribers.[50] Alarmingly, 4 per cent of these children were reported to have experienced online sexual abuse.[51] The abuse typically involved blackmail and solicitation to participate in sexual related activities such as sharing explicit pictures.[52] While the 4 per cent may seem insignificant, it translates to roughly 200 000 children, which is a significant number.

The above statistics highlight the growing reliance on the use of the internet by children, making it an important factor that determines their learning and growth.[53] This makes the internet an important facet through which children's cultural exchange is effected.[54] Given this reliance, there is a pressing need for an inclusive and responsible use of the internet and its related technologies. However, this will require collaboration from the global community and the active participation of all stakeholders to guarantee the safe and secure navigation of children in online platforms globally.[55] It therefore goes without saying that effective child protection in cyberspace should take on board all-important stakeholders in their facets, such as children themselves, parents, educators, the online industry and policy makers, to mention but a few.[56]

47 'Risk and opportunities related to children's online practice' UNICEF *Ghana Country Report* (2017) 10-11.
48 Access to the digital environment for children: Building safer and inclusive digital spaces for refugee children with special needs and disability, https://reliefweb.int/report/world/access-digital-environment-children-building-safer-and-inclusive-digital-spaces-refugee-children-special-needs-and-disability (accessed 12 June 2024).
49 Internet Users Statistics for Africa, https://www.internetworldstats.com/ (accessed 12 June 2024).
50 Rising child abuse cases in Tanzania force review of law, https://www.theeastafrican.co.ke/tea/news/east-africa/tanzania-child-law-3912468/ (accessed 12 June 2024).
51 As above.
52 As above.
53 UNICEF (n 47) 10-11.
54 International Telecommunication Union (ITU) & UNICEF *Guideline for industry on child online protection* (2015).
55 International Cooperation on Child Online Protection, Expert Consultation on ICTs and Violence against Children in Costa Rica, 9-10 June 2014. International Cooperation Child Online Protection
56 Singh & Power (n 40) 100.

4 Protection of children's rights to privacy in cyberspace at global, regional and domestic legal levels

4.1 Protection of children's rights to privacy in the cyberspace at global level

Privacy as a right gets refuge from article 12 of the Universal Declaration of Human Rights (Universal Declaration) of 1948. The Declaration, among other things, discourages arbitrary interference in people's privacy.[57] In similar vein, the International Covenant on Civil and Political Rights (ICCPR) replicates article 12 of the Universal Declaration by obliging states to enact laws to uphold the right of its individuals' privacy.[58] It may be speculatively said that these articles referred to privacy in the traditional physical setting as opposed to the virtual world. This argument is supported by the idea that in 1948 and 1966, when the Declaration and ICCPR were enacted, the level of technology was such that the drafters could not be expected to contemplate the possibilities of what is currently evidenced. That might be the reason that moved the UN later on affirm that any right protected offline is equally protected online.[59]

Alongside the two instruments, there is the UN Convention on the Rights of the Child (CRC).[60] This Convention has received nearly universal acceptance and, arguably, is the most detailed convention in the field of child welfare. However, CRC suffers the same challenge as the Universal Declaration and ICCPR as it was promulgated when children's involvement in cyberspace was still in its infancy and, therefore, it lacked the current technological inputs necessary in upholding children's entitlements in cyberspace.

CRC through article 17 requires states to enable children with information access from different sources within and without the national boundaries, in order to promote their social, spiritual, mental and physical well-being.[61] Under paragraph 9 of General Comment 25 on children's rights in relation to the digital environment, state parties are obliged to create an environment for equal opportunity for children to connect with the online atmosphere and efforts are made to minimise digital exclusion. This includes free and safe access for the children to utilise for education, home and recreational settings.[62]

57 Art 12.
58 Art 17.
59 Resolution 3 of General Assembly Resolution 68/167 was adopted on 18 December 2013.
60 *Adopted by the UN General Assembly on 20 November 1989 and entered into force on 2 September 1990. Tanzania acceded to this Convention on* 1 June 1990.
61 Art 17(1) CRC.
62 CRC Committee General Comment 25 (2021) on children's rights in relation to the digital environment.

In similar vein, state parties to CRC and parents or guardians are obliged to ensure that proper guidelines exist, shielding them from destructive information.[63] It can therefore be argued that it is the spirit of CRC that children should be afforded tools for accessing information and materials across the globe. In the modern era, these tools may include computers, smartphones, tablets and the internet, to mention but a few. It therefore is against the spirit of CRC for governments not to put deliberate measures enabling children's accessibility to the cyberspace enjoying rights such as communication, education and recreation. Additionally, while these children are exercising their rights to exploit the potentials inherent in cyberspace, states in collaboration with guardians have to guarantee that they are free from any harm to their well-being in all facets.

Moreover, CRC in article 12 demands children to be accorded the right to be heard on any matter touching them, relying on the age and the adulthood of the child. Interpreting what 'matters affecting children' means, General Comment 25 states that it means all matters which children's perspectives can improve the quality of the solutions.[64] Arguably, these include enacting laws affecting children or regulating technologies having impacts on their lives.

However, whether or not a child's view should be considered depends on the power of making their opinions, appreciate and evaluate the consequences of the matter, and this has to be taken on after consideration of several factors,[65] given that parents or legal guardians reasonably maintain the control, over their behaviours.[66] This parental responsibility or supervisory right, however, needs to be exercised depending on the evolving capacity of the particular child.[67] Evolving capacity is a concept imported by CRC as a basis for assessing the understanding of the child of the risks in cyberspace independently of their parents or guardians. Parents and guardians are empowered to take charge of that.[68] It is a principle on child's gradual attainment of competencies, understanding as well as agency. CRC under this principle considers the age and development stage of a child as a yardstick for assessing a child's independent engagement from parents and guardians in the digital setting.[69] Therefore, efforts designed to uphold children's privacy rights in their endeavour to access cyberspace should consider the uneven position of children, their competence, understanding, and the associated nature of the risks.[70] Against the above backdrop, it thus is fair to state that it is a violation of CRC to enact laws regulating children's experience in cyberspace without allowing them to air their views on how they want it to be dealt with. Moreover, this is more so because privacy rights of a child are more pressing

63 Art 17(2) CRC.
64 CRC Committee (2009) General Comment 12: The right of the child to be heard para 27.
65 General Comment 12 (n 64) paras 28, 29 & 30.
66 Art 5 CRC.
67 As above.
68 General Comment 25 (2021) on children's rights in relation to the digital environment para 19.
69 As above.
70 As above.

than that of other groups, given the fact that the same are central to their self-identity.[71] State parties should ensure parents and guardians are aware and equally respect children's evolving capacities, autonomy and privacy. They should play a facilitative role in acquisition of digital literacy to children and realisation of their rights, including protection in the digital settings.[72]

Article 16 of CRC prohibits unlawful and arbitrary interference with a child's privacy, including that of his family, and correspondence, and it further requires legal protection against encroachment or attacks on the child's privacy. It has therefore been contended that a child's privacy is threatened by several activities, namely, unregulated data gathering and profiling done by multiplicity of stakeholders, and by the different actions by members of the family. The activities range from sharing photographs or information online by parents or guardians or strangers.[73]

4.2 Protection of children's rights to privacy in cyberspace in Africa

In the African context, upholding children's privacy rights is multi-regulated across several legal instruments, both specific and general, the main instrument being the African Charter on the Rights and Welfare of the Child, 1990 (African Children's Charter). The Children's Charter plays a notable role in safeguarding children's privacy rights in the region. The Charter expresses a child as an individual of less than 18 years of age.[74] Article 12 of the Charter, moreover, guarantees the right of minors to participate in sports and games suitable to their age.[75] This would cover both recreation available online and traditional offline recreations. Despite providing for learning platforms, recreation, social inclusion and civic participation to the young generation, the digital revolution has brought with it new forms of opportunities for harm to children.[76] Moreover, pandemics such as COVID-19 escalated online child abuse and exploitation.[77] These challenges call for a systemic approach as opposed to an issue-based approach.[78]

Under article 10 of the African Children's Charter, a child is protected from arbitrary or unlawful encroachment to their privacy in all its facets.[79] This provision extends to include protection of privacy rights in the cyberspace. This is because international standards require that similar rights that one enjoys

71 CCT261/18 [2019] ZACC 46; 2020 (3) BCLR 245 (CC); 2020 (1) SACR 469 (CC); 2020 (4) SA 319 (CC) (4 December 2019).
72 General Comment 25 (2021) on children's rights in relation to the digital environment para 21.
73 YE Ayalew, V Verdoodt & E Lievens 'General Comment No 25 on children's rights in the digital environment: Implications for children's right to privacy and data protection in Africa' (2024) 24 *Human Rights Law Review* 6.
74 Art 2.
75 Art 12(1).
76 Johnson & Sloth-Nielsen (n 20) 664.
77 As above.
78 Johnson & Sloth-Nielsen (n 20) 665-666.
79 Art 10.

offline should further be enjoyed online.[80] State parties are therefore expected to uphold and guarantee privacy rights in the context of digital communication.[81] Similarly, laws are expected to guarantee and protect privacy online as it does offline.[82] Paragraph 97 of General Comment 25 on children's rights in the digital environment[83] requires regulations relating to the digital environment to be compatible and to keep pace with principles in the offline atmosphere. This means that legislation should afford a similar level of protection to online rights as it does to rights that are enjoyed offline.

Moreover, the African Children's Charter stresses the best interests of the child as the paramount principle in any act performed in relation to children.[84] This principle is dynamic and context-specific and, in assessing it specifically in a digital environment, regard should be had to all children's rights. Under article 4(2) of the Charter, it is against that principle for the government to pass a decision affecting children without affording them a right to air their views directly or through their representatives. Equally, online commercial activities such as advertising and marketing accessible to or targeting children should pay due regard to the genuine opinion of the said children who possibly may be victims or beneficiaries of the activity.[85] Nonetheless, in assessing what amounts to the child's best interests, transparency is of the essence.[86] In the absence of transparency, practices such as profiling, behavioural targeting, information filtering, automated data processing, mandatory identity verification and mass surveillance arbitrary interfere with the child's identity, location, emotions, health, relationships and biometric information, among others.[87] Consequently, this may occasion an everlasting consequence on the child's agency, dignity, health and exercise of their rights.

The only justification for interference with the privacy of children in cyberspace is if same meets the minimum thresholds of being provided by the law, for legitimate purposes, proportionate and designed to observe the best interests of the child, for upholding data minimisation, and should not be inconsistent with the aims and objectives of international standards.[88] Practices such as surveillance and automated processing of children's data, if routinely conducted and if made without parent or guardian consent, are held to be inconsistent with international standards.[89] Therefore, practices such as monitoring of children done for lawful

80 Resolution 3 of General Assembly Resolution 68/167 was adopted on 18 December 2013.
81 Resolution 4 of General Assembly Resolution 68/167 was adopted on 18 December 2013.
82 Resolution (A/RES/71/199) on the right to privacy in the digital age, 2016.
83 CRC Committee General Comment 25 (2021) on children's rights in relation to the digital environment.
84 Art 4.
85 See para 41 of General Comment 25 (2021) on children's rights in relation to the digital environment.
86 See the principal of the best interests of the child.
87 See para 68 of General Comment 25 (2021) on children's rights in relation to the digital environment.
88 See para 69 of General Comment 25.
89 See para 75 of General Comment 25.

and necessary purposes such as safety should be carefully implemented so that it does not prevent a child from enjoying other rights such as access to a helpline and important information.[90] It is suggested that to reduce the risk, programmes hiding child identity while online, such as avatars or pseudonyms, should be employed. These programmes, however, should be carefully handled and should not turn and help in hiding harmful behaviours, especially those that may even come from unscrupulous parents or guardians.[91]

Another significant instrument in Africa is the African Union Convention on Cyber Security and Personal Data Protection, 2014 (Malabo Convention).[92] The Convention intended to guide legislative bodies of member states in enacting legislation on internet security, data protection, cybercrimes and online transactions.[93] The Malabo Convention has not been operative because it has not attained the ratification thresholds.[94] Moreover, Tanzania is yet to be a signatory to the Malabo Convention.[95] The Convention contains some valuable provisions about safeguarding children's abuse or exploitation along with other pertinent rights such as privacy. Article 8(1) obliges state parties to put in place a legal framework that protects data and punishes the violation of privacy rights. Further, article 29(1)(3) protects children against online exploitation by criminalising child pornography. Even though it does not directly address the question of violation of children's data and privacy, this Convention remains relevant in the field of data protection, inclusive of minors' information.[96] It underscores the importance of having an independent authority for preserving of personal information. It unpacks the six principles of data processing without which privacy of personal data cannot be attained. These include consent, lawfulness, fairness, purpose, relevance, storage, confidentiality, accuracy and security. Although it is not currently in force in Tanzania, it continues to serve as a valuable framework for developing robust policies, laws, and institutions that align with international standards on data privacy as a key component of privacy.[97] Nevertheless, sound protection calls for the Tanzanian government to accede to the Malabo Convention as it will be bound by its provisions upon its coming into operation.

90 See para 76 of General Comment 25.
91 See para 77 of General Comment 25.
92 Also known as the Malabo Convention, drafted in 2011, and adopted on 27 June 2014. The Convention has not yet entered into force because under art 36 the treaty will only enter into force after the 15th instrument of ratification or accession has been deposited, but only 5 countries have managed to deposit or accede to this Convention so far.
93 Joseph (n 29) 56.
94 See the List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 29 December 2024).
95 African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 20 December 2024).
96 A model law on data protection (SADC Model Law on Data Protection (2013)) which provides guidance on framing data protection legislation is available for member states.
97 Joseph (n 29) 55.

4.3 Protection of children's rights to privacy under domestic legislation

Tanzania is a signatory to several conventions guaranteeing children's rights and entitlements.[98] Consequently, several pieces of legislation have been enacted for a similar purpose.[99] However, while the adequate safeguard to children's privacy rights in cyberspace requires a robust technologically driven legal and policy regime, the existing policy and legal framework in Tanzania is challenged by the evolving nature of cyberspace. It is therefore argued that with the lack of such comprehensive legal and policy regime tailored towards protecting children's rights to privacy, the protection of children's privacy rights, especially in cyberspace, becomes a mystery.[100] The upcoming part will examine the child protection legal regime in Tanzania and its relevance in guaranteeing children's privacy rights.

4.3.1 Constitution of the United Republic of Tanzania

This is the *grundnorm* establishing the validity of other enactments. The Constitution asserts that any legislation in conflict with it is void to the extent of such contradiction.[101] It may be argued that before the inclusion of the Bill of Rights in the Constitution in 1984,[102] the right to privacy was not explicitly guaranteed, with its protection left to be addressed in other laws such as criminal and property laws.

Among the human right conferred and protected by the Constitution is the privacy rights, in general, and specifically the privacy of communication. Article 16(1) of the Constitution recognises privacy as a right and guarantees various aspects of it, including the privacy of private communication. However, this right is never absolute. Under article 16(2) the right to privacy may be limited under certain circumstances, but with specific reasons and procedures to be established by the law. Notably, the Constitution mandates that any limit to privacy rights must not violate the provisions that guarantee this right. The question of whether the requirements set forth under article 16(2) have been complied with by legislation limiting this right in Tanzania can be answered by an evaluation of each law limiting the right, an exercise falling in the purview of this part.

The right to privacy is further limited by a general clause in article 30(2) of the Constitution. This part prescribes that it is not unlawful to restrain the exercise

98 These include the Convention on the Rights of the Child,1989 and African Charter on the Rights and Welfare of the Child,1990.

99 For example, the Personal Data Protection Act of 2022; the Cybercrimes Act of 2015; the Electronic and Postal Communication Act of 2010.

100 SO Masocha 'Protection of children's rights to privacy and freedom from online exploitation and abuse in Southern Africa. A case study of South Africa and Zimbabwe' Master's dissertation, Makerere University, 2020 4.

101 Art 64(5) Constitution of the United Republic of Tanzania, 1977.

102 See the Fifth Amendment (came into operation in March 1985).

of a right, including the right to privacy, due to purposes such as protecting freedoms and the rights of others, public benefits, morality, defence, peace, safety and health. Essentially, this connotes that privacy rights can be curtailed for these reasons. In the case of *Kukutia Ole Pumpun & Another v The Attorney General & Another*[103] the High Court in interpreting this provision stated that a law restraining any individual right gets refuge under article 30(2) in the event the same meets the thresholds of being lawful in a manner that is not arbitrary. Furthermore, the law should incorporate suitable controls from arbitrary powers and offer an oversight to avoid misuse by those enforcing the law. Lastly, there should not be more restraints than what is essential to accomplish a lawful purpose.

Contextually, the Court's interpretation highlights that, while article 30(2) permits some restraints on the right to privacy, such limitations must meet the three-tiered threshold of legality, proportionality and legitimacy. If a law fails to meet these criteria, it violates article 16 of the Constitution. This implies that article 16(2), which allows laws to limit privacy without violating the Constitution, requires these laws to satisfy the three tests. This decision was further quoted with approval in the case of *AG v Dickson Paul Sanga*,[104] where a provision of a criminal procedural law denying bail to some bailable offences was saved by article 30(2) because it satisfied the proportionality, legitimacy and lawfulness tests. The Court in this case saved section 148(5) of the Criminal Procedure Act because the limit of the right to bail in the purview of this provision passes the above three-tier test. The restraint, therefore, was legal, proportionate and legitimate.

Furthermore, the Constitution under article 18(c) offers personal liberty to communicate and protection from interference in such communication. Unlike article 16(2), this provision contains no claw-back clause, indicating that the liberty to communicate without interference is not subject to legislative restraints. This appears to conflict with the wording of article 16(2), which permits the communication interference for some specific motives. However, article 30(2) seems to resolve this contradiction.

Additionally, the Constitution under article 30(3) allows anyone whose constitutional rights, including privacy rights, are violated or are likely to be violated, to file a suit in the High Court for redress. This provision offers legal recourse for anyone who believes that their privacy rights have been infringed upon. In remedying the infringement, the High Court may order the government to rectify the situation, amend the impugned provision or declare the provision or Act void.[105] However, this provision does not offer pecuniary redress to

103 [1993] TLR 159.
104 Civil Appeal 175 of 2020 (CA).
105 Art 30(5).

the victim, likely leaving this aspect to statutory legislation.[106] Moreover, this provision cannot be exercised if there is another law providing for redress.[107] This would literally mean that because certain laws criminalise acts related to privacy violations, such as interception of communication, this amounts to a redress to bar application of article 30(3). However, criminal liabilities do not always vindicate the victim of the violation. This is probably why article 16 of the Constitution requires the state to enact a law on how privacy can be regulated.

Therefore, the Tanzanian Constitution guarantees privacy rights. As the supreme law, it offers a framework through which laws restraining privacy rights should be premised. These premises to a large extent revolve around minimum safeguards set forth by international instruments such as ICCPR, such as legality, necessity, legitimacy and proportionality.[108] Therefore, it falls upon the statutes allowing limitation of privacy to consider these in their text.

4.3.2 Child Act, 2009

Enacted in 2009, the Child Act is a vital legislation in preserving children's rights in Tanzania. The Act promotes the well-being of children by incorporating the available international and regional standards on children's rights.[109] This Act fosters the welfare of the children by recognising the principle of the best interests of a child under section 4(2), laying the ground for safeguarding minors' privacy rights. In ensuring that personal information relating to children are kept secure, the Act contains provisions that guarantee confidentiality in child care and protection.[110] Despite the inclusion of several rights to be enjoyed by children in the second part of the Act, the right to privacy is not specifically stated. Furthermore, sections 9(3)(a) to (c) of the Act impose several duties and responsibilities on parents, such as protecting children from risks such as abuse, violence, neglect, exposure to physical and moral hazards, discrimination and oppression, but does not extend such duties to protecting children's privacy, particularly in the digital environment.

One of the peculiar features of this Act is the establishment of juvenile courts with the power to hear charges against children and handle children's care applications and maintenance matters.[111] The proceedings before the courts are conducted in a way that upholds the dignity and privacy of the concerned

106 See art 30(4).
107 Sec 8 Basic Rights and Duties Enforcement Act 33 of 1994.
108 UN Human Rights Committee (HRC) CCPR General Comment 16: Article 17 (Right to privacy), The right to respect of privacy, family, home and correspondence, and protection of honour and reputation, 8 April 1988, https://www.refworld.org/legal/general/hrc/1988/en/27539 (accessed 20 December 2024).
109 See the long title.
110 See part II-V.
111 Sec 97.

child.[112] While these courts provide an avenue to address cases where children are suspected of having committed offences, they do not have jurisdiction over violations of children's privacy rights, as their focus primarily is on cases where children themselves have allegedly violated the law.[113] This jurisdictional limitation restricts the scope of legal protection for children's privacy outside criminal or legal conflicts. In summary, while the Act provides a general legal regime for preserving children's rights, it does not explicitly guarantee minors' privacy rights, especially in the online ecosystem. The complementing laws that were expected to cover this void are also lacking. Therefore, this calls for an amendment of the Act to incorporate explicit provisions that guarantee children's privacy rights and extend the jurisdiction of juvenile courts to cover privacy violations.

4.3.3 Personal Data Protection Act, 2022

The Personal Data Protection Act, 2022 (PDPA) was brought in 2022 and came into operation on 1 May 2023. Through its long title, PDPA aims to provide principles for personal data protection, thresholds for the collection and personal data processing, establish an authority to oversee protection of personal information, improve the safety mechanisms for personal information controlled by a multiplicity of stakeholders and offer other related issues. It further aims at preserving the privacy of individuals in its different facets. In so doing, it regulates the gathering and handling of personal data, establishes a structural mechanism to safeguard personal information, protects data subjects and provides remedies thereto.[114]

Section 65 of PDPA gives freedom to data controllers to have in place ethical policies that describe ethics and conducts to be adhered to when collecting or processing personal data. However, the authority established has the power to approve the code of ethics before being operational. With this in mind, the law just sets the objectives and lets the service providers formulate procedures on how to achieve the objectives. The court has commended the practice for taking on board the neutrality of the privacy and data protection sector which cuts across several fields and, therefore, no possibility of a one-fit-all procedure.[115]

Section 23 authorises the collection of data by registered data controllers upon notification to the data subjects of the purposes, recipient, and if the purposes are authorised by the law.[116] This condition may be disregarded in a situation where such data is publicly available or if the data owner authorised collection from a

112 The practice and procedures before the juvenile court are governed by the Law of the Child (Juvenile Court Procedure) Rules, GN 182 of 2016.
113 Sec 98 of the Child Act (Cap 13 RE 2019).
114 Sec 4. The Act came into force on 1 May 2023 and it is complemented by Data Protection (Personal Data Collection and Processing) Regulations, GN 449C of 2023, published on 4 July 2023.
115 *Tito Magoti v Hon Attorney General* (Miscellaneous Civil Cause 18 of 2023) High Court Main Registry at Dar es Salaam.
116 Sec 23(2).

third party. This also applies if giving notice is impracticable, if non-compliance is necessary to comply with other written laws or if giving notice will affect the ground for their collection.[117] These wordings connote that this law authorises the gathering, use and unveiling of one's individual information without procuring permission from the information owner in the circumstances hitherto prescribed. These exceptions may be used as a loophole for violations of privacy specifically in the event the subject is a child. For instance, in a situation where a child's data has been unlawfully published, waiving the duty to seek consent from parents to process them would mean encouraging the unlawful publishing of a child's data. The other risk is in a situation where other written laws allow. The risk comes from the fact that PDPA is the only detailed legislation on safeguarding individual's data in Tanzania. It contains nearly all principles, limitations and minimum thresholds for the safe gathering and handling of personal data. Allowing personal data to be gathered under other laws whose enactments were not meant for security of data puts the right to data security in danger. This opens the doors for actors to opt for other laws whose requirements are not strict and overlook PDPA. The provision would have been protective if it stipulated that such laws must have incorporated similar or higher standard safeguards than PDPA itself. In line with this, in *Tito Magoti v Hon Attorney General*[118] the impracticable circumstances of waiving the requirement to obtain consent were supposed to be listed even if in general terms. The Court held the same about section 23(3)(e) which allows non-compliance with the requirement of consent if doing so would prejudice the lawful purpose of the collection. The lawful purpose ought to be defined to avoid abuse of the provision.

However, the Court ruled section 23(3)(d), which allows non-compliance where it is essential in adherence to other written laws, to be unproblematic. The Court grounded its argument on the fact that since laws are many and change over time, it is difficult to list all of them in a single Act. Much as one may agree with the Court on the fact that it is impossible to list all exceptions, it was prudent for legislators to qualify the statement that such other laws must adhere to the necessary minimum safeguards under PDPA. A blind relief to other laws to allow non-compliance may risk the privacy of personal data because the said other laws do not contain the minimum safeguards as it is in PDPA.

Section 30 imports the conception of sensitive data where the provision disallows the any handling of sensitive personal information unless the subject consents in writing.[119] The Act under section 3 defines sensitive personal information to include data relating to children. The child's consent for data processing should be sought from the parents, guardian, attorneys, heirs or any other person recognised by law as such.[120] However, the requirement of consent

117 Sec 23(3).
118 As above.
119 Sec 30(1).
120 Sec 3.

is waived for several factors such as the requirement of other written laws, for purposes of protecting the child's important right or a third party, if it is essential for a legal claim, if the data is disclosed by the owner, for medical reasons or the interests of the child. Unfortunately, the Act does not define what vital interests of the child are to waive the requirement. In the absence of such meaning, this exception can be abused to the detriment of the child.

Notably, the Act is not explicitly clear on how the written consent envisaged by section 30 should be obtained especially in an online environment. In the USA, for instance, there is a federal law enacted to regulate children's privacy rights, that is, the Children's Online Privacy Protection Act (COPPA).[121] Crucially, COPPA presents the best practice on how consent should be sought and obtained. The Act requires website owners to display downloadable consent forms and parents to authenticate their age and identity.[122]

Moreover, some reasons warranting the revealing of personal data relating to a minor without a genuine authorisation of the parent or guardian are obsolete. For example, provisions such as section 30(5)(d)[123] allow the dealing with minors' data with no consent, merely because the minor himself or herself made the data public. Taking into account the fact that, generally, minors are not in a position to make rational judgments due to immaturity, this exception is unreasonable. The provision should have categorically stipulated that this provision relates to minors who in relation to their evolving capacities can form an independent judgment. This is different in other jurisdictions. For example, in Kenya, the only exception for the data controller to process the child's related data without a parent's or guardian's consent is if it is exclusively for providing counselling or services related to child protection.[124] In South Africa, dealing with individual's information about a child without the consent of a responsible person is if it adheres to an obligation in law. The rest must secure consent or at least sufficient guarantee is provided to ensure non-infringement of the child's privacy.[125]

Likewise, if the intention was that an obligation to notify be waived when the child's data is public owing to their parent's or guardian's act, the same is perplexing as it will mean subjecting a child to a violation of their privacy at the expense of their parent's or guardian's conduct. The situation becomes worse because the law does not require the permission of a parent or guardian to be genuine in terms of being free and informed.[126] This creates chances for ignorant and unscrupulous parents or guardians to consent to the detriment of the child's welfare.

121 Enacted in 1998 and it became operational in 2000. It has been amended from time to time to accommodate technological advancement and the online landscape.
122 See sec 312(5)(b)(i) of the Children's Online Privacy Protection Rule, 1999.
123 See sec 30(5)(d) of the Personal Data Protection Act, 2022.
124 Sec 33(4) of the Data Protection Act 24 of 2019.
125 Sec 35 of the Protection of Personal Information Act 4 of 2013.
126 Sec 2 of the Kenyan Personal Data Protection Act, 2019 defines consent to be the 'manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes'.

The Act remains quiet on its precedence in the event of provisions of other written laws being inconsistent with it in so far as the treatment of individual's data is concerned. The oversight creates room for laws with no minimum safeguards to apply to the detriment of children's rights. At the same time, the Act limits applications of its provisions where other written laws provide for another procedure. For example, section 33(2) relieves the data controller of a burden to communicate to the owner in case the same is under investigation according to other laws. Moreover, section 34(5)(a) is to the effect that the requirement of permission before processing data relating to a minor is immaterial in the event that other written laws provide otherwise.[127] Being a specific Act regulating personal data, it was supposed to take precedence over other written laws in the event of any inconsistency with respect to personal data. This is due to the fact that the Act incorporates necessary safeguards against violations of privacy while processing personal data lawfully when compared to other sector-specific laws.

Nevertheless, the Act bluntly exempts dealing with individual's data contrary to its provisions in any of the following circumstances:[128] if processing is made by the data subject himself for his personal use; if other laws or court orders require; if processing is made to safeguard national safety and security and public interest; if it is made for preventing or detecting crimes; if it is meant to detect or prevent tax evasion; if processing aims at investigating allegations of misuse of public funds and for reasons of vetting for nomination to a position in public service. The provision lacks checks against abuse of the loopholes. The provision should have provided minimum safeguards to any person utilising these exceptions. This has been the practice in international instruments and practices in other states such as Kenya, Uganda and Rwanda.[129]

Section 3 of PDPA defines a 'child' in accordance to the Child Act. Section 4(1) of the Law of the Child Act[130] describes a child as a human below 18 years. Therefore, literally under PDPA, all persons below the age of 18 require parental consent before accessing online platforms for any purpose whatsoever. The question is whether it is reasonable to subject the consent of all children to the consent of a guardian or parent. One may think of a child of 15 to 17 years curtailed with the right of access to online platforms unless their parent formally consents. Some jurisdictions have categorised these children as capable of consenting on their own, subject to the fulfilment of some preconditions.[131] The literatures

127 As an exception to sec 34(1), which requires consent before processing of personal data relating to a child, provides that '[s]ubsection (1) shall not apply where (a) the processing is necessary for compliance with other written laws'.
128 Sec 58(2).
129 See the Data Protection Act 24 Of 2019, Data Protection and Privacy Act, 2019 and Law Relating to the Protection of Personal Data and Privacy Law 58 of 2021.
130 Cap 13 RR 2019.
131 In Spain, eg, the data protection law contains specific provisions on the consent for the processing of data on minors. According to art 13 of the Spanish Personal Data Protection Law, 'data about data subjects over 14 years of age may be processed with their consent, except in cases when the law requires the assistance of parents or guardians'.

demonstrate that in most jurisdictions, the law determines the appropriate age boundary for a minor to consent.[132] This may be the reason why international instruments such as CRC imported the conception of evolving capacities in assessing the power of a child in accessing online platforms independent of their parent or guardian. It can therefore be rightly stated that relying on the general age of majority of the child may be unreasonable and impractical in some situations and environments. It was therefore reasonable, if the evolving capacities of a child was to be employed as a yardstick.

Another pertinent issue relates to the duty of the controller of data to have in place verification processes that guarantee determination of the age of minors and the genuineness of the permission. Age verification is central if the law targets the online services offered straight to children and more so to online services targeting the general audience or mixed audience.[133] This is paramount because surveys show that even the prevailing online service providers that specifically exclude children, such as Facebook, YouTube and Google, minors have been active users while treated as adults in these platforms.[134] In some jurisdictions such as that of Kenya, the law imposes a mandatory condition on the data controller to integrate a suitable mechanism for verifying the age and genuineness of the consent.[135] The contemplated systems are to be determined based upon, among others, the existing technology, the size of information processed, and the likelihood of risk to a child as a result of the processing of their individual information.[136] The highlighted standards are vital in curbing potential abuse of consent by parents, guardians or attorneys. This requirement is not captured in PDPA.

To wind up, PDPA was intended to be a general privacy and individual data safeguard law and it was expected to take precedence over other laws in case of inconsistency. This is because the other laws were not originally enacted to protect privacy or personal data. Therefore, PDPA vaguely warranting disclosure or collection of personal data under such other laws that do not contain the minimum safeguard, makes its enactment futile. The fact that PDPA contains minimum safeguards and preconditions before the disclosure or gathering of individual data, it ought to limit the exercise of other laws to the extent of the minimum standards enshrined therein. Moreover, PDPA should consider incorporating pertinent issues such as evolving capacity and age verification procedure requirements while avoiding blind and obsolete limits to the requirement of the law.

132 M Macenaite & E Kosta 'Consent for processing children's personal data in the EU: Following in US footsteps?' (2017) *Information and Communications Technology Law* 154.
133 Macenaite & Kosta (n 132) 173-174.
134 As above.
135 Sec 33(2) Personal Data Protection Act, 2019.
136 Secs 33(3)(a)-(e) Personal Data Protection Act, 2019.

4.3.4 Cybercrimes Act, 2015

The Act was brought in to establish and regulate crimes associated to the computer system, and information and communications technology. It aimed at providing the procedures to investigate collect and use electronic evidence and related matters.[137] The cyberspace being central to this article makes the Act relevant. The Act makes crimes some computer-related acts having a bearing on personal privacy. It further regulates the accessibility of personal information needed for various purposes such as investigation of crimes. The Act describes a child for the sake of cybercrimes as an individual below 18 years of age.[138]

It moreover criminalises communication, disclosure or transmission of computer data to unauthorised persons. Equally, the law makes it unlawful for one to intentionally receive unauthorised computer data.[139] The offence is punishable with a fine. Alternatively, one may be imprisoned for one year or both. The Act creates an offence of data espionage. This relates to obtaining any computer data that is subject to protection against access without permission.[140] The contravention of this provision is punishable by a fine. The convict may alternatively serve a sentence of incarceration or both incarceration and fine. The offences do not make a distinction between the general data from some sensitive data such as that of children once unlawfully interfered with or unlawfully obtained.

The Act makes it unlawful to publish through computer systems or facilitate access to child pornography through computer systems.[141] This is an interesting move by the Act as it sets apart child pornography from those involving adults. The offence bears a punishment of not less than a fine of 50 million shillings or thrice the value of unjust benefits received by the convict. Incarceration of seven years and above or both fine and incarceration and a fine may be imposed. The provision displays the seriousness in addressing the problem by imposing a heavier punishment than it imposes on pornography involving adults.[142]

4.3.5 Electronic and Postal Communication Act, 2010

The Electronic and Postal Communication Act (EPOCA) is the main enactment in electronic communication whose intention, among others, was to keep abreast with developments in the electronic communications industry.[143] One

137 See the long tile to the Cybercrimes Act 14 of 2015.
138 Sec 3.
139 Sec 7(2).
140 Sec 8.
141 As above.
142 See punishment for the offence of pornography under sec 14.
143 See the long title of the Electronic and Postal Communication Act 3 of 2010. The Act came into force on 7 May 2010 and it repealed and replaced the Broadcasting Services Act, 1993.

of its objectives was to address challenges brought about by new technology.[144] First, the law obliges owners of a mobile SIM card to register it with the service provider[145] by submitting the subscriber's personal information.[146] It is believed that with such information the holders can monitor the communications of respective subscribers.[147] Section 98 obliges the service providers to maintain confidentiality of whatever personal information they acquire from subscribers.[148] This obligation is not reflected in the Tanzania Communications Regulatory Authority (TCRA) despite them having the power to retain a subscriber's information from service providers.[149]

Section 120 criminalises all conduct associated with communication interception such as interception, attempted interception or procuring another to encroach electronic communications,[150] disclosure or attempt to disclose information obtained by interception[151] and the use of the information obtained through interception.[152] However, nowhere does the Act attempt to vindicate the victim. EPOCA authorises the interception of communication and provides the duty of confidentiality to service providers' agents. The Act makes offences related to privacy such as any disclosure of intercepted communication by authorised persons.

Moreover, it limits service providers from accessing the communication for quality control purposes. Nevertheless, the law excludes TCRA from exercising confidentiality, something that puts the privacy of subscribers in jeopardy. It can, therefore, be argued that despite authorising interception of communication under other laws, it does not put in place adequate safeguards for privacy rights. Therefore, by doing so, it encourages unlawful interception by criminal investigators. Furthermore, this law fails to enlist the procedural mechanisms on how authorised individual may encroach such communication. This contravenes the constitutional provision of article 16(2) and that of article 17 of ICCPR which necessitates any law restraining privacy rights detail processes such as ways to challenge any misuse of such restriction and the redress possibility. ICCPR requires that in the event a communication is to be encroached, neutral authority should exist to authorise, and there must exist processes describing the environments, degree, and ways in which the work may be carried out and the remedy in the event the procedures have not been adhered ro by the responsible persons. The principles put forth by this Act do not give due regard to children and, therefore, protection enshrined therein is general.

144 Makulilo (n 30).
145 Sec 93(1) of the Electronic and Postal Communication Act 3 of 2010 and Regulation 4(1)(a) of the SIM Card Registration Regulations GN 112 of 2020.
146 Sec 93(2).
147 Makulilo (n 30) 4.
148 Sec 98(1).
149 Sec 91.
150 Sec120(a) of the Electronic and Postal Communication Act 3 of 2010.
151 Sec 120(b).
152 Sec 120(c).

4.3.6 Media Services Act, 2016

The Act was meant to provide promotion for professionalism in the media industry, to establish a board of accreditation for journalists, independent media council, and regime for regulating media services and other related matters.[153] Section 7(3)(f) of the Act obliges all media houses, while executing their responsibilities, to ensure that information aired out does not, among other things, involve unwarranted encroachment of an individual's privacy. Section 7(4) provides that the sub-part in this Act that regulates ownership, rights and obligations of media houses supersedes any provisions under any other written law in the event of inconsistency. This obligation concerns all online platforms.[154]

An analysis of the domestic legal framework has shown that, currently, several loopholes can be used by perpetrators to violate children's rights to privacy. As hitherto shown, some Acts provide general protection of privacy rights without giving due regard to the sensitivity of minors' privacy rights, while others provide obsolete or blind exceptions that may be abused against the interests of children's privacy rights. Others do not incorporate important issues such as the evolving capacities and age verification requirements. However, the highlighted shortfalls are not at all surprising. This is because legislation in middle and low-income countries has often trailed important technological advancement.[155] In that regard, the problem of legislating in the digital environment is well noted.

5 Role of the court in the protection of children's rights to privacy

The Constitution of the United Republic of Tanzania entrusts the judiciary of Tanzania with all judicial powers.[156] It is the judiciary that has the final powers in the dispensation of justice in Tanzania.[157] Therefore, when children's rights are violated, they have the right to seek appropriate remedies through established legal channels.[158] Principle 5 of the General Principles on Children's Online Privacy and Freedom of Expression acknowledges the complexity of achieving effective remedies, especially in a digital environment. It acknowledges that the availability of effective remedies depends on, first, a robust system of redress that ensures smooth resolution of complaints filed by children and their guardians; second, a transparent reporting mechanism that aligns with their digital literacy levels; and, third, the existence of avenues for further review or redress. However,

153 See the long title of the Media Services Act, 2016.
154 See the definition of media house, media services and media under sec 3.
155 M Hightower 'The Fourth Amendment and the dark web: How to embrace a digital jurisprudence that protects individual liberties (2021) *Georgetown Law Journal Online* 179.
156 See art 4(2).
157 See art 107B (1) of the Constitution of the United Republic of Tanzania,1977 as amended from time to time.
158 See CRC Committee General Comment 5 and Human Rights Committee General Comment 5.

the realisation of these rights is contingent upon the existence of a robust legal framework designed to preserve minors' rights. In the absence of a comprehensive and technologically driven legal framework tailored towards protecting children's privacy rights in Tanzania, this responsibility becomes the exclusive province of the courts. This vital role stems from articles 107A and 107B of the Constitution, which recognise courts as the guardians of citizens' rights.

In embracing their constitutional roles and mandates, Tanzanian courts have been instrumental in vindicating children's rights, especially those involving sexual violence and exploitation. Such cases have garnered significant court attention. The case of *Job Mlama & 2 Others v R*[159] serves as an example. In this case the appellants were charged with sexual exploitation contrary to section 138B(1)(e) of the Penal Code. It was alleged that the appellants jointly and together used violence to procure the child aged 13 years for sexual intercourse with a dog. In upholding its role in protecting children's rights and by acknowledging the victim's vulnerability as a child, the Court found the appellant's action inhumane and a serious violation of human rights.

In certain limited circumstances, the courts have also demonstrated sensitivity to children's rights by prioritising the right to privacy and the best interests of a child. In the case of *Kuruthum Omary Kahiba & Another v Mwajuma Omary Kahiba*[160] the Court considered privacy concerns when a minor sues for paternity. It was stated that, in such cases, the Court must prioritise the right to privacy and the best interests of a child. Additionally, in all criminal proceedings involving children, Tanzanian courts have consistently been showing respect for children's privacy while remaining mindful of their mandate and role in child protection. For example, in the case of *Sadick Hamad Ndiunze v The Republic*,[161] having noted that the victim was under the age of majority, the Court proposed to hide her actual name throughout the judgment for good reasons of preserving her respective integrity and privacy rights. It is worth commenting that this practice has consistently been applied by Tanzanian courts in all cases involving children.[162]

However, despite these notable developments, courts in Tanzania have not obtained enough avenues to vindicate children's rights to privacy outside criminal cases that relate mostly to child exploitation and abuse. This is because courts do not proactively seek matters to adjudicate unless parties are before it. Consequently, our courts have not yet tried a case where purely the violation of a child's privacy is at issue. This may be attributed to a low level of awareness of citizens' rights to privacy, which leads to a failure to understand the implications

159 Criminal Appeal 222 of 2012 [2013] TZCA 333 (30 July 2013) (unreported).
160 Misc Civil Cause 4 of 2018) [2020] TZHC 3597 (29 September 2020) (unreported).
161 Criminal Appeal 35 of 2022 [2023] TZHC 20683 (14 August 2023) (unreported).
162 See, eg, the case of *Kaimu Said v Republic* Criminal Appeal 391 of 2019 [2021] TZCA 273 (7 June 2021) and *Francis Petro v Republic* Criminal Appeal 534 of 2016 [2019] TZCA 304 (27 August 2019).

it has on the victim's well-being.[163] Moreover, the constitutional petitions filed in the High Court challenging provisions violating the right to privacy, generally, have often been unsuccessful on either technical or constitutional grounds.[164]

Several factors may be cited as the obstacles preventing the courts from fulfilling their role and mandate. First, unlike in disputes pertaining to children's mistreatment, there exists limited referral of cases to courts involving violations of children's rights to privacy. This limitation stems from ignorance of both children and parents about this important right.[165] Additionally, there is a lack of effective means for reporting and channelling children's claims, partly due to the existence of reporting systems such as Child Online Protection (COP) that do not adequately cover children's privacy issues and offer prompt responses to complaints filed by children. Second, since violations of children's privacy rights touch upon constitutional rights, they must be addressed by the High Court through constitutional petitions. The complex procedures involved in filing constitutional petitions in Tanzania deter children and their guardians from seeking redress.[166] For these reasons, the court's role in developing minors' rights jurisprudence is counselled.

On the contrary, other jurisdictions such as the Kenyan experience offer a good example of the role the courts can play in advancing children's rights to privacy in the online setting. The courts have so far been taking a progressive stance in affirming such rights by laying down legal principles that contribute to the advancement of children's rights jurisprudence. This is evident in numerous court decisions where children's rights to privacy were vindicated. A recent Kenyan case of *CMM & 6 Others v Standard Group & 4 Others*[167] suffices to illustrate the active part played by the Kenyan Supreme Court in protecting children's privacy rights. In this case, seven children were charged with arson. When the matter was called for hearing, the respondents, through their media outlets and platforms, publicly aired and published images and names of the children. The central issue was whether the alleged published images and names of children facing criminal charges, violated the children's privacy rights and that the acts by the respondents were not in the minors' best interest. In its considered judgment the Court decided that the acts by the respondent were violative of the appellants' privacy rights and the right for their best interests to be considered, as guaranteed under articles 31(c) and 53(2) of the Kenyan Constitution, respectively.

163 CIPESA 'Privacy and personal data protection in Tanzania: Challenges and trends' (2018) *State of Internet Freedom in Africa* 13, https://cipesa.org/download/reports/State-of-Internet-Freedom-in-Tanzania-2018.pdf (accessed 26 December 2024).

164 Eg, the case of *Magoti* (n 115).

165 S Shannon 'Protecting children's right to privacy in the digital age: Parents as trustees of children's rights' (2020) 36 *Children's Legal Rights Journal* 174.

166 See the Basic Rights and Duties Enforcement Act (Cap 3 RE 2019) and Basic Rights and Duties Enforcement (Practice and Procedure) Rules, 2014.

167 *CMM (suing as next friends of and on behalf of CWM) & 6 Others v Standard Group & 4 Others* Petition 13 (E015) of 2022 [2023] KESC 68 (KLR) (8 September 2023) (Judgment).

The Kenyan courts have also affirmed children privacy rights, stressing the importance of procuring consent before using children's images. In the case of *NWR & Another v Green Sports Africa Ltd & 4 Others*[168] the petitioner filed the petition against the respondents for violation of her children's rights to privacy after the respondents had taken and published the children's photographs without consent. Having found that the consent of the minor's parents or guardians was neither sought nor obtained, the Court ruled the act to be unlawful and a violation of the petitioner's constitutional rights.

The experience of Kenyan courts, therefore, highlights three crucial roles that the court can play in preserving children's privacy rights in the virtual setting. First, the court can define the boundaries of the constitutional right to privacy. Second, through bold pronouncements, it can establish a framework for addressing privacy complaints and developing jurisprudence to efficiently address infringement of children's privacy rights. Third, the courts can address current disparities in the legal framework, thereby shaping the landscape of children's rights jurisprudence.[169] Tanzanian courts, therefore, are urged to embrace these roles to fill the current gaps in the legal framework, a step that will be vital in moulding the legal landscape for children's rights in Tanzania.

6 Conclusion

This study has shown that children's privacy rights, especially in the virtual settings in Tanzania, are a critical issue that requires concerted efforts for their protection. The traditional legal framework in Tanzania has been challenged by the evolving nature of cyberspace, making children's privacy rights protection a nightmare. This calls for more robust and technologically driven legislation to make such protection a reality. Despite Tanzania's efforts to protect children through various legislative and policy initiatives, such initiatives still fall short of tackling the drawbacks brought up by the online ecosystem. The Personal Data Protection Act, the Cyber Crime Act, the Child Act and the Electronic and Postal Communication Act contain several loopholes that allow the violation of children's privacy in cyberspace. For example, in all these laws there is no requirement for internet service providers to implement age verification mechanisms. Therefore, the need for Tanzania to update its legal and policy structure on children's protection online emerges. Additionally, while it may be acknowledged that the adequate safeguard to children's rights largely hinges on the inclusion of all main partakers, children placed at the centre, their involvement in Tanzania has been minimal resulting in the formulation of laws that are not informed with the realities on the ground. It is thus argued that, in a bid to enhance its legal protection for children's rights, Tanzania needs to take on

168 [2017] eKLR.
169 NC Breen 'An analysis of the role of the courts in selected child protection cases: Jurisprudence and remedy' Master's dissertation, University of Pretoria, 2017 6.

board all key stakeholders and formulate laws that incorporate international best practices and standards, ensuring that children in Tanzania enjoy the same level of privacy as their peers worldwide. Cross-border cooperation is also essential especially when the violation has international implications. TCRA is also urged to observe the statistical growth of children's involvement in cyberspace. Considering the sensitive nature of children's online privacy and the essence of safeguarding it, tracking their navigation trends in cyberspace is paramount.