African Journal on Privacy & Data Protection

To cite: GA Arowolo 'Safeguarding the rights to privacy and digital protection of children in Africa: Nigeria and South Africa in focus' (2025) 2
African Journal on Privacy & Data Protection 126-152
https://doi.org/10.29053/ajpdp.v2i1.0007

Safeguarding the rights to privacy and digital protection of children in Africa: Nigeria and South Africa in focus

*Grace Ayodele Arowolo**
Associate Professor and Acting Head, Department of Public and Private Law, Lagos State University, Ojo, Lagos, Nigeria

Abstract

In its General Comment 25 (2021), the United Nations Committee on the Rights of the Child encourages state parties to ensure the protection and upholding of children's rights on the internet. To achieve this, a strong legislative framework is required. Therefore, this article aims to examine the degree to which children's rights to privacy and data protection are incorporated and enshrined into the Nigerian and South African regulatory frameworks. These countries are state parties to various regional and international laws that safeguard the rights of children. The article also aims to explore relevant legislation in the European Union (EU) and the United States of America, as both are assumed to contain comprehensive provisions for protecting the right to privacy of children and protection from online abuse. The purpose is to compare the US and EU laws with the Nigerian and South African laws, detect deficiencies and/or best practices, and the key regulatory and implementation challenges of their legal frameworks. The article adopts a doctrinal approach that enables the analysis of

* BL (Lagos) LLB (Hons) (Ife, Ile Ife) LLM (Lagos State University) PhD (Ambrose Alli); ayodelearowolo2006@yahoo.com; grace.arowolo.edu.ng

various applicable international, regional and national legal frameworks in South Africa and Nigeria. The article finds, among others, that, although both countries have made notable progress in enacting laws safeguarding the rights of children offline and online, the legal frameworks of these countries do not adequately safeguard children's rights to privacy in the online ecosystem. The article argues that with weak legislation, the effective protection of children's right to privacy and their participation in the digital space may be negatively affected. Hence, a reform of the relevant laws is crucial in the two countries, and children should be consulted in the process as they possess the statutory right to be engaged in issues that concern them.

Key words: children; right to privacy; digital protection; Nigeria; South Africa

1 Introduction

In the modern digital age, numerous daily activities produce data, often without immediate awareness. In addition to the information shared, additional data is collected via sensors or derived using advanced algorithms.[1] This circumference results in a complex interplay between digital data processing and the freedoms designed to uphold the right to personal data protection and the right to privacy.[2] While digital technologies provide new avenues for exercising human rights, they are frequently abused to infringe upon human rights generally. Key concerns include digital identity, the use of surveillance technologies, data protection and privacy, and online violence and harassment.[3]

The internet and mobile technologies are a vital aspect of many children's lives.[4] Globally, 79 per cent of individuals aged between 15 to 24 use the internet.[5] In affluent and developing countries, and progressively in lower-income nations, children's activities are increasingly reliant on mobile and online networks, making it nearly impossible to distinguish between online and offline experiences.[6] This integration of offline and online experiences brings about a variety of digitally-driven risks and opportunities.[7] While some have emerged in the digital era, most are influenced by children's inherent needs, abilities, and

1 C Caglar 'Children's right to privacy and data protection: Does the article on conditions applicable to child's consent under the GDPR tackle the challenges of the digital era or create further confusion?' (2021) 12 *European Journal of Law and Technology* 1-31.

2 S Livingstone, M Stoilova & R Nandagiri 'Children's data and privacy online: Growing up in a digital age: An evidence review' (2019), https://eprints.lse. ac.uk/id/eprint/101283 (accessed 5 June 2024).

3 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* 1-24.

4 M Stoilova, S Livingstone & D Kardefelt-Winther 'Global kids online: Researching children's rights globally in the digital age' (2016) 6 *Global Studies of Childhood* 455-466.

5 International Telecommunication Union (ITU) 'Facts and Figures 2023', https://www.itu.int/itu-d/reports/ statistics/ 2023/10/10/ ff23-youth-internet-use/#:~:tex (accessed 4 July 2024).

6 Livingstone and others (n 2).

7 EJ Helsper and others 'Country classification: Opportunities, risks, harm and parental mediation' (2023), https://eprints.lse.ac.uk/52023/ (accessed 24 July 2024).

susceptibilities.[8] The emergent opportunities for children include the utilisation of new recreational and social media as sites of learning, including peer-based learning; the accumulation of social and technological skills for participation in today's world; and variety in media literacy and online engagements, which may offer advantages for socialisation and education, preparing individuals for future social and professional environments.[9] Most of the risks that children might encounter relate to social media violence such as sexual predation and grooming, cyberbullying, 'sexting' and harassment.[10]

Thus, the digital era has created both challenges and opportunities in advancing children's rights worldwide.[11]

Threat to children online constitutes an infringement on their privacy and protection from abuse and exploitation.[12] Children are more susceptible to interferences in their privacy because of their inability to comprehend the long-term effects of disclosing personal data online.[13] Further to the foregoing, children seek assurances against commercial exploitation and have urged governments to enact laws that safeguard their information and limit industry monitoring of minors online.[14] Several years earlier, Livingstone and others advocated a new General Comment from the United Nations (UN) Committee on the Rights of the Child (CRC Committee). This is as a result of the risks children face in online environments and the vast opportunities they may be denied, the rapidity of change and the fact that 'digital' is not about to go away.[15]

Consequently, in 2021 the CRC Committee adopted General Comment 25, which explains how state parties should enforce the Convention on the

8 L Raftree & K Bachan 'Integrating information and communication technologies into communication for development strategies to support and empower marginalised adolescent girls' (2013), https://www.Researchgate.net/publication/330135273_Integrating_Information_and_Communication_Technologies_into_Communication_for_Development_Strategies_to_Support_and_Empower_Marginalized_Adolescent_Girls?. (accessed 20 July 2024).

9 C Samuels and others 'Connected dot com: Young people's navigation of online risks: Social media ICTs and online safety' Cape Town, South Africa: Centre for Justice and Crime Prevention and UNICEF (2013) 11-12.

10 As above.

11 I Milkaite & E Lievens 'The internet of toys: Playing games with children's data?' in G Mascheroni & D Holloway (eds) *The internet of toys: Practices, Affordances and the political economy of children's smart play* (2019) 285.

12 OM Sibanda '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, University of Pretoria, 2019/2020 2.

13 UNICEF 'Children's online privacy and freedom of expression' (2018), https://www.guvenliweb.org.tr/dosya/ ZybsG.pdf (accessed 15 May 2024).

14 A Third & L Moody 'Our rights in a digital world: A report on the children's consultations to inform UNCRC General Comment 25' (2021), https://5rightsfoundation.com/uploads/OurRIghtsinaDigitalWorld-FullReport.pdf (accessed 23 May 2024).

15 S Livingstone, G Lansdown & A Third 'The case for a UNCRC General Comment on children's rights and digital media' Report prepared for Children's Commissioner for England, 28 June 2017, London School of Economics (LSE) 1-63.

Rights of the Child (CRC),[16] pertaining to the digital landscape.[17] CRC is the first international instrument with legally binding force to encompass the comprehensive scope of children's human rights.[18] These include the right to privacy (article16); the right to attain and enjoy the highest possible standard of health (article 24); the right to an adequate standard of living that supports the child's social, mental, physical, and spiritual development (article 27); and the right to education (article 28).

General Comment 25 addresses, among other things, the general principles of CRC, that is, the rights of children to equal treatment provided in article 2 of CRC; the child's utmost welfare in article 3; the right to survival, life and development in article 6; and the recognition of the child's perspectives in article 12. The General Comment advanced other rights enshrined in CRC, such as the right to privacy in article 16 of CRC; freedom of expression in article 13; and protection from commercial exploitation in article 32.

One of the measures proposed by the General Comment is for state parties to 'review, adopt and update national legislation in line with international human rights standards, to ensure that the digital environment is compatible with the rights set out in the Convention'.[19]

This article seeks to address how well South Africa and Nigeria have adhered to the recommendations of General Comment 25. The article establishes that the regulatory frameworks of Nigeria and South Africa do not effectively safeguard children's right to privacy and protection from online abuse and exploitation. Hence, the article recommends law reform. The article draws best practices from the legal regimes of the European Union (EU) and the USA to inform law reform. It also makes other recommendations.

2 Understanding the concept of privacy and data protection

Privacy is a basic right crucial for human dignity and autonomy, functioning as the cornerstone for many other rights.[20] It enables the creation of limitations and management of thresholds for protection from unjustified intrusion into people's lives.[21] Data protection is typically defined as legal provisions aimed at

16 Adopted by General Assembly Resolution 44/25 of 20 November 1989.
17 UN Committee on the Rights of the Child General Comment 25 on children's rights in relation to the digital environment' (2021) UN Doc CRC/C/CG/25 dated 2 March 2021.
18 UNICEF 'A summary of the rights under the Convention on the Rights of the Child', https://www.unicef.org/ montenegro/en/reports/summary-rights-under-convention-rights-child, (accessed 5 January 2025).
19 UNICEF (n 18) para 23.
20 Privacy International 'What is privacy', https://privacyinternational.org/explainer/56/what-privacy (accessed 24 June 2024).
21 As above.

safeguarding personal information.[22] A robust data protection framework can empower individuals, curb harmful data practices and prevent data exploitation, playing a crucial role in establishing effective governance structures both nationally and globally.[23]

Article 16 of CRC prohibits the illegal intrusion into children's family life, privacy, home, or communications, and illegal assaults on their reputation and honour. Although a right to 'data protection' is not clearly stated in article 16, General Comment 25 aims to broaden and guide the interpretation of the article provision in CRC.

General Comment 25 summarised the importance of Children's right to privacy in the online space as follows:[24]

> Privacy is vital for children's agency, dignity and safety, and for the exercise of their rights. Threats to children's privacy may arise from their own activities in the digital environment, as well as from the activities of others, for example by parents' sharing online the photos or other information of their children, or by caregivers, other family members, peers, educators or strangers. Threats to children's privacy may also arise from data collection and processing by public institutions, businesses and other organizations; as well as from criminal activities such as hacking and identity theft.

3 Opportunities and risks relating to children's participation online

Digital technology is often regarded as a major game changer of our time, with the potential to transform the lives of the most underprivileged and at-risk children of the world by enabling them to grow, learn, and reach their full potential.[25] Digitalisation enables children with disabilities to interact with others and make independent choices, grants access to education for those in marginalised or remote places and, in humanitarian crises, assists displaced children in finding safe routes and reconnecting with their families.[26] Increased digital connectivity among children has created fresh opportunities for civic participation and social integration, offering the possibility of disrupting cycles of poverty and deprivation;[27] furthers the promotion of their right to education[28]

22 Privacy International 'A guide for policy engagement on data protection: Data protection explained', https:// privacyinternational.org/sites/default/files/2018-09/Part%201%20%20Data%20Protection%2C%20Explained.pdf (accessed 30 June 2024).
23 As above.
24 General Comment 25 (n 17) para 108.
25 UNICEF 'The state of the world's children 2017: Children in a digital world' (2017), https:// www.unicef.org/ media/48581/file/SOWC_2017_ENG.pdf (accessed 12 August 2024).
26 As above.
27 As above.
28 S Livingstone, J Carr & J Byrne, 'One in three: Internet governance and children's rights' Innocenti Discussion Paper 2016-01 United Nations Children's Fund UNICEF 1-36.

and freedom of expression;[29] grants them access to information important for their well-being, including their reproductive and sexual health;[30] grants them the opportunities to develop skills in coding, creating, and sharing information and such opportunities as are available on the internet.[31] Children can also play games, listen to music and watch movies online, thereby enjoying their right to leisure and recreation.[32]

However, It is crucial to emphasise the digital divide, which has prevented some children from benefiting from the advantages provided by the internet for different reasons.[33] According to the United Nations Children's Fund (UNICEF), strong inequality in digital connectivity is evident globally and across the world's regions.[34] Based on 2023 statistics, 98 per cent of youths (individuals aged between 15 to 24 years) in Europe have access to the internet, while in Asia Pacific, 81 per cent of youths, also between ages 15 and 24, have home internet connectivity.[35] However, only 53 per cent of youths aged between 15 and 24 in Africa can access the internet.[36] African children encounter multiple intersecting challenges, such as financial limitations, restricted online literacy, and issues linked to gender and race.[37] For example, in Nigeria, adolescent girls have limited modern employment skills and fall behind in internet access and usage (21 per cent compared to 38 per cent for boys),[38] although both added together remain low.

Although internet access has created opportunities for children, it also poses risks of violating their rights online.[39] One of the major risks confronting children in the online space is the infringement of their right to privacy and protection from exploitation and abuse[40] by the use of technologies through tracking, broadcasting and monitoring children's live images, locations or behaviours.[41] Image-based abuse, cyberbullying and exposure to inappropriate content or harmful advice can lead to negative experiences, including disconnection from

29 Livingstone and others (n 15).
30 As above.
31 As above.
32 Sibanda (n 12).
33 As above.
34 UNICEF & International Telecommunication Union (ITU) 'How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic' UNICEF New York, 2020.
35 International Telecommunication Union (ITU) 'Facts and figures 2023', https://public.tableau.com/app/profile/ ituint/viz/ITUFactsandFigures2023/InternetUse05 (accessed 3 January 2025).
36 As above.
37 African Children's Committee 'Day of general discussion: Children's rights in the digital world – A concept note', https://www. acerwc. africa/en/article/activity/day-general-discussion-childrens-rights-digital-world (accessed 24 November 2022).
38 UNICEF 'Country office annual report 2022: Nigeria – 321', https://www.unicef.org/media/142201/file/Nigeria-2022-COAR.pdf (accessed 25 June 2024).
39 Council of Europe Commissioner for Human Rights 'Protecting children's rights in the digital age: An ever-growing challenge' (2014), www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen... (accessed 24 May 2024).
40 Sibanda (n 12).
41 UNICEF 'Children's online privacy and freedom of expression' (Industry toolkit, UNICEF 2018) 8, www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf (accessed 24 May 2024).

reality, emotional distress, anxiety, depression, suicidal thoughts, sexual or physical assault, self-harm and reputational damage.[42]

4 Analysis of states' responsibilities under CRC according to states' interpretation of General Comment 25

General Comment 25 was adopted in the realisation that the digital environment plays a crucial role in various aspects of children's lives, including periods of crisis, as well as in societal functions such as governmental services, commerce and education, which increasingly depend on digital technologies.[43] The General Comment expatiates on the specific positive obligations of states in safeguarding children's rights in online space, including updating or enacting legislation, implementing all-encompassing strategies and policies, and enabling autonomous oversight and investigations by national human rights agencies, and the enforcement of mechanisms to safeguard children from risks, including cyber aggression and online and child sexual abuse and exploitation facilitated by technology.[44]

Article 16 of CRC provides for privacy rights of children as discussed above. The CRC Committee outlines how state parties should apply the Convention in online spaces and offers guidance on policy, legislative, and other mechanisms to ensure absolute compliance with their duties under the Convention and its Optional Protocols. This guidance considers the risks, challenges and opportunities involved in promoting, protecting, fulfilling and respecting all children's rights in online spaces.[45]

The most extensive section in General Comment 25 focuses on the right to privacy. Paragraph 67 of General Comment acknowledges the fact that 'threats to children's privacy may arise from data collection and profiling by public institutions, businesses and other organisations', but equally 'from the activities of family members, for example, by parents sharing photographs online or a stranger sharing information about a child'.

Paragraph 68 highlights various online activities that depend on data processing, including compulsory identity authentication, profiling, extensive monitoring and behavioural targeting. The Committee believes that these practices may result in unlawful or arbitrary infringements on the privacy rights of children. With respect to states' obligations to uphold the privacy rights, paragraph 70 of General Comment 25 states that states must enact and implement data protection laws that include exclusive safeguards for children

42 D Mitra 'Keeping children safe online: A literature review' (2020) Centre for Excellence in Child and Family Welfare Melbourne 1-21.
43 General Comment 25 (n 17) para 3.
44 General Comment 25 (n 17) paras 22-49.
45 General Comment 25 (n 17) para 7.

while ensuring that other rights, such as their rights to play and their rights to freedom of expression, are not arbitrarily restricted.[46]

General Comment 25 also advocates a legal prohibition on specific online activities, such as neuromarketing, consumer-specific advertising and commercial profiling.[47] It acknowledges the duty of states to provide adequate guidance and support to caregivers and parents in fulfilling their child-upbringing obligations. This necessitates the advancement of awareness raising[48] and educational programmes that provide information on protecting children's privacy, targeting several stakeholders, including care givers, parents, children, policy makers and the general public.

The General Comment also emphasises the necessity to respect children's developing capabilities and independence, urging states to support parents in upholding a reasonable balance between their duties and the child's rights.[49] Parents and care givers should be guided in this balancing process by the best interests of the child and the recognition of their evolving capabilities. States are urged to educate care givers, parents, children and the public on the significance of the privacy rights of a child and how certain parental actions may violate this right. When care givers and parents monitor a child's online activities, they should do so proportionately and with utmost regard for the child's evolving capabilities.[50]

5 African regional framework

5.1 African Charter on the Rights and Welfare of the Child

Just like article 16 of CRC, article 10 of the African Charter on the Rights and Welfare of the Child (African Children's Charter)[51] protects children's rights to privacy, home or correspondence, reputation and honour. A major departure of this provision from CRC is the inclusion in its article 10(3) the provision that 'parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children'. However, this was clarified by the African Committee of Experts on the Rights and Welfare of the Child (African Children's Committee) in its General Comment on article 31 of the African Children's Charter espousing that the rationale for the provision is to balance the authority exercised over children by adults with children's responsibility to show respect

46 As above.
47 General Comment 25 (n 17) para 42.
48 General Comment 25 (n 17) para 21.
49 General Comment 25 (n 17) para 86.
50 General Comment 25 (n 17) para 76.
51 OAU/CAB/LEG/153/Rev 2 1990. Nigeria ratified the African Children's Charter on 23 July 2001.

and consideration for that authority.[52] The General Comment further states that the 'rights of the child including freedom of expression, participation, and development, among others, shall not be compromised or violated by reference to "respect for adults"'.[53] Thus, it is essential to recognise that privacy rights of children should not be compromised or infringed upon due to the provision on parental control in article 10(3).[54] The African Children's Charter did not make any provisions for data protection.

5.2 African Union Convention on Cyber Security and Personal Data Protection

The African Union (AU) Convention on Cyber Security and Personal Data Protection (Malabo Convention) is Africa's first regional framework on data protection.[55] Article 8(1) of the Convention mandates state parties to enact regulatory frameworks that reinforce basic rights and freedoms, especially data protection, and to impose sanctions for any breach of privacy.[56] Under article 8(2), any form of data processing should respect basic rights and freedoms. The Convention contains no provision for the handling of data concerning children, but article 29(3) guarantees safeguarding children from exploitation and abuse in online spaces while urging state parties to criminalise child pornography. Article 29(3) provides as follows:

> State parties shall take the necessary measures to ensure that, in case of conviction, national courts will give a ruling for confiscation of materials, equipment, instruments, computer program, and all other devices or data belonging to the convicted person and used to commit any of the offences mentioned in the Convention including child pornography.

Nigeria is not yet a party to this Convention, while South Africa is a signatory.

5.3 Southern African Development Community Model Law on Data Protection and Information and Communications Technology 2013

The law upholds children's privacy as it provides that the personal data of a child can be processed only in accordance with article 37 of the Model Law, which states that 'if a child is the data subject, his or her rights may be exercised by his

52 African Children's Committee General Comment on article 31 of the African Charter on the Rights and Welfare of the Child on the responsibilities of the child' (2017) African Union Commission, Addis Ababa, Ethiopia 1-34.

53 As above.

54 A Singh & T Power 'Understanding the privacy rights of the African child in the digital era' (2021) 21 *African Human Rights Law Journal* 99-125.

55 O Babalola 'Data protection legal regime and data governance in Africa: An overview' (2023) AERC Working Paper DG-003 African Economic Research Consortium, Nairobi, Kenya 1-27.

56 Adopted by the 23rd ordinary session of the Assembly held in Malabo, Equatorial Guinea 2014. Nigeria has neither signed nor ratified the Convention. South Africa signed the Convention on 16 February 2023 but is yet to ratify it.

or her parents or legal guardian' except as per national laws, the child has the capacity to give consent individualistically according to their ability and age, in line with internationally accepted standards that require recognising the evolving capabilities of children. This provision complies with the African Children's Charter discussed above and paragraphs 70 and 71 of the General Comment which interprets CRC.

5.4 African Union Child Online Safety and Empowerment Policy 2024

This policy seeks to identify gaps and areas requiring harmonisation to uphold children's rights and to address cross-border challenges.[57] The goals of the policy include enhancing and harmonising national, regional and continental legal and regulatory frameworks on online safety of children; recognising the advantages of, and responses to, current and growing threats to children's identity, privacy, and agency in the online space; and developing a unified multi-stakeholder framework to address online risks for children, particularly child sexual abuse and exploitation.[58]

The policy's key recommendations include reinforcing high-level governmental commitments to child online safety; enhancing criminal justice systems to enhance law enforcement and for the judicial arm of governments to effectively combat child online safety offences including exploitation and sexual abuse of children in online spaces; and advancing and advocating accessible digital education in schools and among guardians, parents and community stakeholders.[59]

6 Compliance with General Comment 25 recommendations on the right to privacy: Nigeria and South Africa

This part examines the degree to which children's rights to privacy are protected in the digital environment in Nigeria and South Africa, based in light of the provisions of paragraph 70 of General Comment 25 concerning the obligations imposed upon states to adopt robust legislation that safeguards children's right to data protection and privacy.

At the international level, the origin of the right to privacy has been traced to the Universal Declaration of Human Rights (Universal Declaration).[60] Article 12 of the Declaration prohibits the subjection of anyone to the illegal interference with their privacy. Article 17 of the International Covenant on Civil and Political

57 Adopted by the 44th ordinary session of the African Union Executive Council in February 2024 in Addis Ababa, Ethiopia.
58 As above.
59 As above.
60 Universal Declaration of Human Rights 1948.

Rights (ICCPR)[61] forbids arbitrary interference with citizens' privacy. Apart from CRC examined above, these international laws do not make specific mention of children's data protection rights.

7 Nigeria's legal framework

Nigeria is bound by the provisions of the Universal Declaration on right to privacy and is also a party to ICCPR. Other laws and regulations that impact on data protection and privacy in Nigeria include CRC, the African Children's Charter and the General Comment discussed above, as well as the following:

7.1 Constitution of Nigeria

Section 37 of the Nigerian Constitution guarantees 'the privacy of citizens (children inclusive) to their homes, correspondence, telephone conversations and telegraphic communications'.[62] In *Nwali v Ebonyi State Independent Electoral Commission*[63] the Nigerian Court of Appeal broadly interpreted this provision to encompass all facets of human life, thus, tracing the origin of data protection in Nigeria to the privacy provisions guaranteed by the Nigerian Constitution.[64]

With specific reference to privacy rights of children, Nigeria is also a party to CRC[65] and the African Children's Charter[66] which were domesticated to the Child's Right Act (CRA) in 2003.[67] Section 8 of the CRA states that '[e]very child has the right to his privacy, family life, home, correspondence, telephone conversation and telegraphic communications'. As in the African Children's Charter, section 8(3) of the CRA subjects the exercise of children's right to privacy to adequate supervision and oversight by their parents and legal guardians. The provisions of these instruments, including the Constitution, make no specific reference to the safeguarding and respect for children's privacy in the online space.

7.2 Nigerian Data Protection Act 2023

One of the major objectives of the Nigerian Data Protection Act (NDPA) in its section 1 is to protect the basic rights, interests and freedoms of data subjects, as enshrined in the Constitution of the Federal Republic of Nigeria, 1999 (as

61 General Assembly Resolution 2200A (XXI) 1966.
62 Constitution of the Federal Republic of Nigeria 1999 (as amended).
63 (2014) LPELR – 23682 (CA).
64 O Babalola 'Nigeria's data protection legal and institutional model: An overview' (2022) 12 *International Data Privacy Law* 41-52.
65 Adopted by General Assembly Resolution 44/25 1989. Nigeria ratified CRC on 19 April 1991.
66 African Children's Charter (n 51).
67 Child's Right Act 26 of 2003.

amended). Under section 65 of the Act, a child is an individual under the age of 18 years.[68] According to sections 31(1) and (2) of the Act, when the data subject is a child or an individual without legal competence to give consent, the data controller must obtain consent from the legal guardian or parent, as applicable, before processing the child's data. Furthermore, the data controller must implement appropriate procedures to confirm consent and age, taking into account the available technology. However, under section 31(5) of the Act, the Nigeria Data Protection Commission (NDPC) is empowered by the NDPA to establish regulations for protecting children aged 13 and above in relation to accessing information and services electronically upon the explicit request of the child.[69] Thus, with respect to the processing of data from children in the age group of 13 years and above but under the age of 18, guidelines need to be issued from the regulatory agency since, as stated in section 64 of the NDPA, regulations established before the NDPA came into effect shall remain valid unless they conflict with the NDPA or are repealed.[70] This implies that, if a child is above the age of 13, the recommendation of the General Comment would apply. This means that, when a child is mentally matured to understand the consequences of online activities and able to give consent, they can be allowed to give such consent with or without their legal guardian. Section 65 is the definition section of the Act.

The NDPA currently is the primary legislation on data protection in Nigeria, superseding the NDPR. The NDPA will prevail in the event of any conflict with any other regulations.

7.3 Cybercrimes (Prohibition, Prevention, etc) Act 2015

Some of the sections of this Act have been amended by the Cybercrimes (Prohibition, Prevention etc) (Amendment) Act 2024 but the provision on child pornography remains intact. The Act safeguards children against child pornography and other related offences. Section 23 of the Act prohibits the procurement, production, transmission, possession and distribution of child pornography in any data storage device or a computer system, making such actions as offences. Upon conviction, the penalty for such actions is a 10-year prison term or a fine of N20 000 000.00 or both. In contrast, obtaining child pornography for oneself or another person, as well as owning child pornography on a data storage medium or in a computer system, carries a maximum penalty of five years' imprisonment or a fine of up to N10 000 000.00 or both.

Section 23(2) prohibits and penalises soliciting, grooming or proposing, via any computer network or system, to meet a child with the intention of having

68 This is in accordance with the definition of a child in sec 277 of the Child's Right Act.
69 Sec 31(5) NDPA 2023.
70 Sec 64(2)(f) NDPA.

sexual relations with the child. Likewise, the Act punishes the production, transmission, distribution or ownership of child pornography. This implies that sexual conversations with a minor, luring a minor into engaging in child pornography, or committing other acts that aim to exploit a child in the digital space, constitutes a violation of the child's rights, which can be enforced against the perpetrator.[71] However, section 23 of the Cybercrimes Act 2015 did not specifically mention children's rights to privacy in the digital space.

In Nigeria, the legislative framework regulating a child's right to digital privacy is still imperfect. Although there are laws governing general data protection of citizens, children are scarcely mentioned and the few provisions on children are not comprehensive compared to other jurisdictions discussed below. There are other laws, although not primarily focused on data protection, that contain provisions that influence and govern data protection in specific contexts,[72] namely, the Freedom of Information Act 2011;[73] the National Health Act 2014;[74] the HIV and AIDS (Anti-Discrimination) Act 2014; and the National Information Technology Development Agency Act 2007.[75] However, it does not specific provision for privacy rights of children in the digital world.

8 South Africa's legal framework

Just like Nigeria, South Africa is bound by the Universal Declaration and ICCPR. South Africa is a party to CRC[76] and the African Children's Charter.[77] The relevant national laws include the following:

8.1 The Constitution

The right to privacy is generally recognised as a basic human right in the Bill of Rights of the Constitution of South Africa.[78] Section 14 of the Constitution provides for everyone's right to privacy, including 'the right not to have (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed'. Section 28 safeguards children's rights and the paramountcy of their best interests in every matter that affects them. Section 14 applies to children and is broad enough to include their privacy right in the digital realm as it states 'communication'.

71 MB Adisa 'A child's right in the digital environment: Legal considerations', https://www.mondaq.com/nigeria/privacy-protection/1285096/a-childs-right-in-the-digital-environment-legal-considerations (accessed 15 January 2025).
72 ICLG 'Data protection laws and regulations in Nigeria 2024-2025', https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria (accessed 12 July 2024).
73 CAP F43 Laws of the Federation of Nigeria 2011.
74 Act 8 of 2014.
75 Sec 6(c) Cap N156 Laws of the Federation of Nigeria 2010.
76 CRC (n 16). South Africa ratified the Convention in 1995.
77 African Children's Charter (n 51). South Africa ratified the Charter in 2000.
78 The Constitution of the Republic of South Africa, 1996.

8.2 Children's Act 38 of 2005

The Children's Act[79] complements the rights of children enshrined in the South African Constitution. Section 1 defines abuse to include bullying, sexual abuse and subjecting or exposing a child to actions that may be detrimental to them. The section further defines commercial sexual exploitation as the recruitment of a child to engage in sexual activities in exchange for money or other rewards, including pornography and prostitution. These forms of abuse though not explicitly addressed defined in the Act can be linked to harmful acts perpetrated on the internet.

The Children's Act 38 of 2005 is currently being amended to better align with the data protection and privacy rights of children in South Africa.[80] This is a specific requirement of the General Comment on children's privacy protection in the online space. It is hoped that the amendment will be finalised.

8.3 Protection of Personal Information Act

The objectives of the Protection of Personal Information Act (POPIA) include the advancement and safeguarding of personal information processed by private and public entities and the Promotion of Access to Information Act, 2000.[81] Section 34 of the Act forbids the processing of personal data of children by any responsible party except as stated under section 35 when, among others, the processing is conducted with the prior consent of a competent individual; it is essential for the enforcement, exercise, or protection of a legal right or duty; required to abide by an obligation under international public law; or intended for research, statistical, or historical purposes. From the above provisions, it is clear that the Act does not permit the handling of personal information of another person without their consent and provides stringent, additional protection to children in section 35. However, section 35 also creates a limitation as to when children's data may be processed. It can be assumed that where the processing of information is not one of the exceptions listed in section 35, the personal information of a child cannot be allowed for processing. It has also been posited that there is still significant uncertainty regarding how POPIA will regulate the processing of children's information.[82]

79 Children's Act 38 of 2005.
80 Centre for Human Rights *A study on children's right to privacy in the digital sphere in the African region* (2022) 1-57.
81 Protection of Personal Information Act 4 of 2013 (POPIA).
82 POPIpack 'Unpacking the processing of children's information in terms of POPI', https://www.popipack.co.za/unpacking-the-processing-of-childrens-information/ (accessed 12 January 2025).

8.4 Films and Publications Amendment Act 2019

The aims of the Act include the amendment of the Films and Publications Act, 1996, in order to amend and insert certain definitions; make provision for the composition, establishment and selection of members of the Enforcement Committee; expand the compliance obligations under the Films and Publications Act, along with the adherence and oversight responsibilities of the Film and Publication Board, to include online distributors; strengthen the regulation of the classification of games, publications, and films; and provide for accreditation of independent commercial online distributors by the Film and Publication Board.[83]

Section 18(G)(1) criminalises the production, creation or distribution by any person 'in any medium, including the internet, and social media any films or photographs depicting sexual violence and violence against children'.[84] It is an offence under section 24(A)(4)(a) and section 24(3)(j) for anyone to permit children access to a game, publication, or film rated 'X18', including granting children access to scenes of explicit sexual conduct. Furthermore, registered film or game distributors may, provided an exemption is granted by the South African Film and Publication Board, distribute a game or film classified as 'X18' online, subject to conditions such as ensuring that children are unable to access such a game or film online. Section 24B criminalises child pornography.[85]

8.5 Criminal Law (Sexual Offences and Related Matters) Amendment Act 2007

This Act makes comprehensive provision for children's protection against sexual offences, including offences related to grooming or sexual exploitation, and the production of child pornography, although the offences are similar to the offences created for adults, with the aim of addressing the particular vulnerability of children.[86] Section 10 prohibits and criminalises the display or exposure of child pornography to adults, while section 19 criminalises the exposure or display of child pornography to children. Sections 17 and 18 prohibit the sexual exploitation of children for monetary or other gain and grooming of children respectively. Under section 20, it is also a crime to derive a benefit from or use a child for child pornography. However, the Act has been criticised for creating sexual offences that largely overlap with those created in the Films and Publications Act.[87] The provision of the Criminal Law Amendment Act, however,

83 The Films and Publications Amendment Act 11 of 2019.
84 As above.
85 As above.
86 Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007.
87 SS Terblanche & N Mollema 'Child pornography in South Africa' (2011) 24 *South African Journal of Criminal Justice* 286.

is acceptable since the aims and objectives of the Act are different from that of the Films and Publications Act.

8.6 Cybercrimes Act 2020

In terms of section 3 of the Cybercrimes Act,[88] the illegal interception of data is an offence, while the unlawful distribution of data messages is an offence under section 14. Section 15 also makes it an offence for a person to make an unlawful and intentional data message that threatens persons with damage to property or violence. Section 24 of the Act gives South African courts jurisdiction over any act or omission alleged to constitute an offence under the Act and that affects an individual in South Africa, even if the defined cybercrime occurs outside the country.

Pursuant to the Cybercrimes Act, litigations involving children's protection have been brought before the courts. For example, in *SM v ABB*[89] the father of the child had shared content from her WhatsApp chat (as well as her mother's) during a divorce case. The child's mother filed an application to prevent the father (respondent) from further accessing and distributing both her (the applicant's) WhatsApp messages and emails, as well as those of their minor child.

The Court ruled that the respondent's behaviour in accessing the applicant's and the minor child's messages violated their right to privacy: The information was shared with the medical practitioner and the headmaster solely to create a cognitive bias in their minds against the applicant and potentially the minor.

The case indicates that parental rights to access the child's digital communications without justification may be restricted with respect to a child's privacy rights. It also portrays South Africa's efforts in protecting privacy rights online.

Furthermore, in *S v Stevens*[90] the accused, Stevens, was involved with two young girls, who were five years old at the time of the incident. He was accused of removing the underwear of the girls while they were asleep for the purpose of taking photographs, and in certain instances touching their private parts with his fingers. Approximately 71 photographs were taken of the children. He was convicted on two counts of indecently assaulting the girls and eight counts of creating and possessing child pornography in contravention of sections 27(1)(a)(i) and (ii) of the Films and Publications Act 65 of 1996. The regional magistrate handed down a sentence of eight years' imprisonment to the accused, of which three years were suspended. Upon appeal to the High Court of Eastern Cape

88 Cyber Crimes Act 19 of 2020.
89 Case 20/1732 (11 September 2020, Gauteng Local division).
90 (2007) JDR 0637 (E). 188 [2014] 2 SACR. CA & R54/07.

Province, the sentence was modified to six years' imprisonment, with two years suspended.

In *S v Kleinhans*[91] a 74 year-old businessman, Kleinhans, was charged with numerous counts of sexual offences against underaged girls. Most of the charges involved capturing photographs of a complainant, a young girl who was between the ages of 13 and 14 years, while she was either only partially clothed or naked. The appellant was charged with an offence of producing child pornography which he was able to do through producing nude pictures of a child complainant in contravention of section 24(B)(1)(b) of the Films and Publications Act 65 of 1996, and the provisions of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007 (the Act) which prohibits, among others, the manufacture of child pornography in section 20(1), sexual grooming of children in section 18(2)(a) of the Act and sexually assaulting the complainant (a child) by fondling her breasts in section 5(1) of the Act.

The magistrate sentenced the accused to 15 years' imprisonment. Upon appeal to the High Court of South Africa, Western Cape Division, the 15-year prison sentence was overturned and substituted with an effective term of imprisonment for four years, with an additional suspension of four years.

South Africa has also made many efforts in adopting policies and laws that recognise the safeguarding of children's privacy online, and has taken a step further by signing the Council of Europe Convention on Cybercrime, the first international treaty on offences committed through the internet and other computer networks.[92] Being an observer to the Convention, South Africa has the privilege and ability to participate in the activities and discussions relating to the Convention without being legally bound. However, it lacks the ability to vote or propose solutions to the challenges of the Convention.[93] South Africa was the sole African nation to take part in the negotiations for the Council of Europe Convention on Cybercrime.[94] Consequently, the South African government has implemented various laws addressing cybercrime and incorporating substantive legal provisions from the Council of Europe Convention.[95] Most notable in this regard is the Electronic Communications and Transactions Act 25 of 2002 (ECT Act), the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013.[96]

91 (2014) 2 SACR.
92 Council of Europe 'Fight against cybercrime' (2015), https://www.europewatchdog.info/en/treaties_and_ monitoring/ cybercrime/ (accessed 12 August 2024).
93 T Reinsman 'International organisations or institutions, observer status', https://opil.ouplaw.com/display/ 10.1093/ law:epil/9780199231690/...(accessed 12 January 2025).
94 Council of Europe 'Cybercrime', https://www.coe.int/en/web/cybercrime/-/octopus-project-benchmarking-the-implementation-of-the-south-african-cybercrimes-act-in-line-with-the-international-best-practice... (accessed 10 January 2025).
95 Council of Europe 'South Africa', https://www.coe.int/en/web/octopus/-/south-africa (accessed 10 January 2025).
96 As above.

Nigeria has acceded to the Council of Europe Convention since 6 July 2022.[97] However, the failure to enshrine digital protection in the extant child right protection laws in Nigeria and South Africa suggests that the countries still have much ground to cover. Therefore, law reform through amendments to existing frameworks to address new risks is hereby suggested.

9 The legal framework for safeguarding children's privacy and data protection in other jurisdictions

For this purpose, the European Union (EU) and the United States of America (USA) have been selected.

9.1 European Union

The EU has been rated as having one of the broadest data privacy protection frameworks globally and is regarded as a pacesetter and catalyst of data privacy protection laws.[98] The data protection framework explicitly acknowledges that processing children's personal data requires special safeguards and offers strengthened protection for such data,[99] although the General Data Protection Regulation (GDPR) of the EU considered below does not specifically provide for their protection 'offline'. Both South Africa and Nigeria also have explicit provisions for safeguarding children online, as examined earlier in this article. The Nigerian NDPA is much more detailed on their online protection than the GDPR. The wording of the provisions of the EU framework is as discussed under the European Union Primary Laws below. European law protecting children's rights is largely based on CRC.[100]

9.1.2 European Union primary laws

The EU provides for the safeguarding of both the right to data protection and right to privacy.[101] First, article 16 of the treaty on the functioning of the EU provides that 'everyone has the right to the protection of personal data concerning them'.[102] Article 7 of the Charter of Fundamental Rights of the European Union 2000 (CFREU) established the citizens' right to privacy by stating that

97 N Ayitogo 'Nigeria signs Budapest Convention on Cybercrime', https://www.premiumtimesng.com/news/top-news/550037-nigeria-signs-budapest-convention-on-cybercrime.html?tztc=1 (accessed 15 January 2025).
98 AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2 *International Data Privacy Law* 163-178.
99 Lexis Nexis 'EU GDPR – Children and data protection law', https://www.lexisnexis.co.uk/legal/guidance/eu-gdpr-children-data-protection-law (accessed 14 January 2025).
100 European Union Agency for Fundamental Rights and Council of Europe *Handbook on European law relating to the rights of the child* (2022) 26.
101 Milkaite & Lievens (n 3).
102 European Parliament 'Understanding EU data protection policy', https://www.europarl.europa.eu/RegData/ etudes/BRIE/2020/651923/EPRS... (accessed 15 January 2025).

'everyone has the right to respect for his or her private and family life, home and communications'.[103] Article 8 recognises the right of everyone to the protection of their personal data, which has to be handled lawfully and fairly for stipulated purposes, either with the person's consent or on another legal basis.

Importantly, article 24 of CFREU expressly recognises the right of the child to protection, essential for their well-being, and to freely share their opinions on issues affecting them, in line with their maturity and age, whereas in all matters involving children, their best interests must be a foremost consideration.[104]

9.1.3 General Data Protection Regulation

The EU adopted a specific provision in the General Data Protection Regulation (GDPR)[105] to tackle issues regarding the processing of children's data.

Under article 1, the subject matter and objectives of the GDPR were stated. It 'lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data'. The GDPR contains several provisions specifically designed to protect the rights of child data subjects. Recital 38 of the GDPR recognises that children require special protection concerning their personal data, given the fact that they may not be as aware as adults of the consequences, risks, safeguards, and their rights regarding data processing. According to the recital, such special protection is particularly essential when collecting children's data for profiling and marketing purposes.[106]

Regarding the lawfulness of data processing, article 6(1)(a) mandates that the data subject gives consent to the processing of their personal data. Under article 8(1) of the Regulation, the processing of the personal data of such child shall be lawful 'where the child is at least 16 years old'. If the child is under the age of 16, this kind of processing must be deemed lawful only 'if consent is given or authorised by the holder of parental responsibility over the child'.[107] Such consent, however, is not required in the context of counselling or preventive services provided directly to a child.[108] By law, member states may provide for a lower age not below 13 years.[109]

103 Charter of Fundamental Rights of the European Union (CFREU) (2000/C 364/01).
104 As above.
105 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016) L 119/1.
106 Milkaite & Lievens (n 3).
107 As above.
108 Recital 38 GDPR.
109 Art 8(1) GDPR.

Article 12 of the GDPR requires the processing of data to be 'concise, transparent, intelligible and in an easily accessible form, for any information addressed specifically to a child'.[110]

Article 17 of the GDPR provides the data subjects with the right to erasure ('right to be forgotten') of personal data concerning them, among others, when the personal data is no longer needed, or the data subject revokes the consent upon which the processing is based or objects to the processing. Generally, article 7(3) of the GDPR states that it 'shall be as easy to withdraw consent as it is to give it'. However, the right to erasure is not absolute and may be overridden, for instance, when required to uphold the right to freedom of information and expression.[111] Its most significant limitations stem from the necessity to balance erasure with freedom of expression and the public interest, as outlined in article 17 of the GDPR.[112]

Similarly, in Nigeria, section 34(1)(d) of the NDPA examined above provides for a data subject's right to erasure, while section 24 of South Africa's POPIA equally provides that there may be a request from a data subject to the controller to amend or remove their personal data. This will be helpful to children whose consent was ignorantly given or who want their information removed for any reason. Generally, however, the GDPR does not specifically provide for their protection 'offline'. Also, both South Africa and Nigeria have explicit provisions for the protection of children online, mentioned in this article. In fact, the Nigerian Act is much more detailed on their online protection than the GDPR.

10 United States of America

The United States adopts a sectoral approach to data privacy regulation, as it lacks an all-encompassing federal law that regulates the privacy and protection of personal data.[113] The statutes are applicable only to specific sectors such as 'healthcare, education, communications, and financial services or, in the case of online data collection, to children'.[114]

110 As above.
111 Information Commissioner's Office 'How does the right to erasure apply to children?', https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children... (accessed 15 January 2025).
112 S Grossi 'The right to erasure: To be or not to be, forgotten?', https://www.byarcadia.org/post/the-right-to-erasure-to-be-or-not-to-be-forgotten (accessed 20 January 2025).
113 SM Boyne 'Data protection in the United States' (2018) 66 *American Journal of Comparative Law* 299-343.
114 N Terry 'Existential challenges for health care data protection in the United States' (2017) 3 *Ethics, Medicine and Public Health* 21.

10.1 Children's Online Privacy Protection Act of 1998

Although the United States has not ratified CRC, it adopted the Children's Online Privacy Protection Act (COPPA)[115] in 1998 and has since acquired extensive expertise in implementing it in practice.[116] COPPA governs the collection and use of data collected from children under 13 by websites and mobile applications. Section 1301(1) defines a child as a person below the age of 13. Section 1303 prohibits unfair and deceptive acts for gathering and processing children's personal information online. An operator or online website is required to secure verifiable parental authorisation for collecting, disclosing, or using children's personal information under section 1303(b)(A)(ii) except where the online contact information collected from a child is used solely to respond once (on a singular basis) and directly, to a particular request from the child and is neither retained in a retrievable form nor used for further contact by the operator under section 1303(2)(A), or a request for online contact information or a parent's or child's name, solely for the purpose of securing parental consent under section 1303(2)(B).

10.2 Children and Teens' Online Privacy Protection Act

On 7 July 2024 the US Senate passed the Children and Teens' Online Privacy Protection Act (COPPA 2.0)[117] and the Kids Online Safety Act (KOSA) to better protect teens and children online.[118] The aim is to amend the Children's Online Privacy Protection Act of 1998 to enhance safeguards for the online use, collection and disclosure of personal information of children and teenagers, along with other related objectives. COPPA 2.0 prohibits online companies from obtaining personal information from users under the age of 17 years without their authorisation. It prohibits targeted advertising to teenagers and children and introduces a button to eraser, allowing parents and children to delete personal information online.[119] When in full force, this will aid better protection of children's privacy protection online.

115 The Children's Online Privacy Protection Act (COPPA) is a US federal law that was adopted in 1998 and became applicable in 2000.

116 Milkaite & Lievens (n 3).

117 118th Congress 1st session 'In the Senate of the United States', https://www.markey.senate.gov/imo/media/doc/coppa_20_in_118th_-_050323pdf.pdfhttps://www.markey.senate.gov/imo/media/doc/coppa_20_in_118th_-050323pdf.pdf (accessed 10 August 2024).

118 US Senate Committee on Commerce Science and Transportation 'Senate overwhelmingly passes children's online privacy legislation' Press Release, 30 July 2024, https://www.commerce.senate.gov/2024/7/senate-overwhelmingly-passes-children-s-online-privacy-legislation (accessed 12 August 2024).

119 US Senate Committee on Commerce Science and Transportation 'Kids online privacy protections – finally – set to pass Senate', https://www.commerce.senate.gov/2024/7/kids-online-privacy-protections-finally-set-to-pass-senate (accessed 12 August 2024).

10.3 Children's Internet Protection Act

The Children's Internet Protection Act (CIPA) was passed by Congress in 2000 to address issues regarding children's exposure to harmful or obscene content online.[120] CIPA imposes particular requirements for schools and libraries that receive discounted internet access or internal connections through the E-rate programme, a programme that helps make certain products and communication services more affordable for eligible institutions.[121] Libraries and schools subject to CIPA are ineligible for E-rate programme discounts unless they certify the implementation of an online safety policy incorporating technology protection measures.[122] The protective measures must filter or restrict internet access to images that are (a) obscene, (b) classified as child pornography, or (c) harmful to minors (when accessed on computers used by minors). Schools subject to CIPA must meet two additional certification requirements: (i) their internet safety policies must incorporate monitoring of minors' online activities; and (ii) they must educate minors on proper behaviour when on the internet, including communications on social networking websites, in chat rooms, and awareness of as well as response to cyberbullying.[123]

Libraries and schools subject to CIPA must establish and enforce an internet safety policy that addresses various concerns, including minors' access to indecent online content, their security and safety while using chat rooms, email, and other direct electronic communications, as well as unauthorised access, such as 'hacking' and other illegal online activities by minors.[124]

10.4 The United States Code

The United States Code (USC) is a compilation of a number of public laws presently valid and in force, organised by subject matter. The Code is organised into 54 titles, by subject area, further divided by section and chapter. The US Code also contains provisions for online protection of children in America.[125] The following online activities are prohibited under the US Code:

120 Federal Communications Commission 'Children's Internet Protection Act (CIPA)', https://www.fcc.gov/sites/ default/files/childrens_internet_protection_act_cipa.pdf (accessed 12 August 2024).
121 As above.
122 As above.
123 As above.
124 As above.
125 United States Senate 'The United States Code', https://www.senate.gov/pagelayout/legislative/one_item_ and_teasers/usCode_page.htm (accessed 13 August 2024).

10.5 Sexual exploitation of children (production of child pornography)

Section 2251 title 18 of the Code[126] prohibits the induction, enticement or coercion of a minor to be involved in conduct that is sexually explicit for purposes of creating visual depictions of such conduct. Attempts or conspiracy to commit child pornography is an offence that is subject to prosecution under federal law.[127] Section 2256 defines child pornography as any visual portrayal of sexually-explicit behaviour involving a minor (an individual under the age of 18). Under that section, visual depictions encompass videos, photographs, computer-generated or digital images that are indistinguishable from a real minor, as well as images that have been created, altered or adapted, but appear to show a recognisable, real minor.[128] Under federal law, unprocessed videotape, undeveloped film, and digitally stored data that has the potential to be converted into visual images of child pornography are also considered unlawful visual depictions.[129]

Child pornography attracts stiff penalties. For instance, in *US v James Snyder*[130] the accused was convicted for producing, receiving, distributing and possessing child pornography and sentenced to 168 months' imprisonment followed by six years of supervised release. In *US v Donald Blakley*[131] the accused was convicted on a 15-count charge for conspiracy to knowingly receive and distribute visual portrayals of a minor engaged in conduct that is sexually explicit and sentenced to approximately seven years and three months' imprisonment.

10.6 Cyberbullying

Section 223(a)(1)(B) of title 47[132] makes it an offence to knowingly use a telecommunications device to produce, generate, initiate or solicit the transmission of any comment, proposal request, image, suggestion, or other obscene communication, including child pornography, with the knowledge that the recipient is under 18 years of age.[133] Further, harassing any individual or repeatedly using a telecommunications device to initiate communications with the intent to harass constitutes an offence punishable by up to two years' imprisonment, a fine, or both.[134]

126 Criminal Division US Department of Justice 'Citizen's guide to US federal law on child pornography', https:// www.justice.gov/criminal/criminal-ceos/citizens-guide-us-federal-law-child-pornography (accessed 13 August 2024).
127 As above.
128 As above.
129 As above.
130 (2005) 239 F 229.
131 222 USC sec 2252B(d) title 18.
132 Legal Information Institute (LII) '47 US Code § 223 – Obscene or harassing telephone calls in the district of Columbia or in interstate or foreign communications', https://www.law.cornell.edu/uscode/text/47/223 (accessed 10 August 2024).
133 As above.
134 As above.

10.7 Obscene visual representations of the sexual abuse of children

Section 1466A of title 18[135] prohibits any person from knowingly creating, receiving, possessing or distributing with the intent to transfer or distribute visual representations, including paintings, cartoons or drawings, which depict minors appearing to engage in conducts that are sexually explicit and are considered obscene.[136] Any individual who attempts or conspires to commit the act shall also be deemed guilty of the offence.[137] Section 1470 of title 18 prohibits the transfer or attempted transfer of material that is obscene to a minor who is below the age of 16 using the US mail or any means of foreign or interstate commerce.[138] It is illegal for a person to deliberately use interactive computer services to display obscene material, making it available to a minor below 18 years,[139] and knowingly making a commercial communication through the internet, including obscenity, available to any minor.[140]

10.8 Coercion and enticement

Under section 2422(b) of title 18[141] it is a criminal offence for any individual to knowingly use any facility, the mail or any means of foreign or interstate commerce, or to act within the special territorial or maritime jurisdiction of the United States, to entice, induce or coerce a person under the age of 18 to engage in prostitution or any sexual activity. An attempt to do so is also an offence. Upon conviction, the offender shall be fined and sentenced to a minimum of 10 years' imprisonment or for life.[142]

11 Gaps in the Nigerian and South African legal frameworks

Based on the analysis of the legal frameworks for safeguarding the protection of children's data and privacy online in the EU and the United States, it is observed that some gaps exist in the legal and regulatory frameworks of South Africa and Nigeria.

An overview of the regulatory framework for safeguarding children's privacy rights in Nigeria above indicates that some of the legislations are not adapted

135 Legal Information Institute '18 US Code § 1466A – Obscene visual representations of the sexual abuse of children', https://www.law.cornell.edu/uscode/text/18/1466A... (accessed 11 August 2024).
136 As above.
137 USC sec 1446A(2)(B) title 18.
138 18 USC 1470: 'Transfer of obscene material to minors', https://uscode.house.gov/ view.xhtml?req= granuleid: USC-prelim-title18-section1470&num=0&edition=prelim (accessed 9 August 2024).
139 USC sec 223(d) title 47.
140 USC sec 231 title 47.
141 Legal Information Institute (LII) '18 US Code § 2422 – Coercion and enticement', https://www.law.cornell.edu/ uscode/text/18/2422 (accessed 9 August 2024).
142 As above.

to the digital environment. Although the National Data Protection Act, 2023 regulates the manner of processing of children's data, it is mainly concerned with parental consent without making comprehensive provisions for child's privacy online protection as it exists especially under the US laws considered above.

Despite the foregoing, Nigeria has made much more progress than South Africa through the incorporation of more robust provisions for the protection of children's privacy online via section 31 of the NDPA. Section 31 requires data controller(s) to obtain the consent of the parent or guardian and also verify the age of a child using identification documents approved by government before processing the data of any child. In South Africa, section 35 of POPIA requires that consent of a competent person be obtained before processing a child's data, but unlike the NDPA, it does not explicitly require the responsible party to verify the age of the child. The Nigerian Cybercrimes Act discussed above also safeguards children against child pornography and other related offences. However, the provisions of these laws need to be expanded to comprehensively address the safeguarding of children's data. The expansion can be done through law reform wherein necessary provisions such as in the US laws are incorporated into them. With regard to South Africa, the provisions of the Sexual Offences Legislation and the Films and Publications Act also safeguard children from online abuse and exploitation as they address issues of exploitation of children, child pornography, online grooming and the exposure of children to harmful content. The Protection of Harassment Act also protects children from online harassment. However, both countries, Nigeria and South Africa, still need to take steps to review their laws in line with the recommendations of the CRC Committee's General Comment 25 discussed above, taking inspiration also from the US laws.

12 Recommendations

In order to safeguard the rights to privacy of children and ensure their freedom from online abuse and exploitation, in compliance with General Comment 25, the following recommendations are made:

(1) The existing laws, especially the CRA and NDPA of Nigeria and the Child Law of South Africa, should be reviewed to comprehensively enshrine provisions similar to those in the USA laws so as to come in tune with current global realities in the digital realm, the exposure and the attendant risks posed to children online. This also ensures compliance with General Comment 25's prescription in its paragraph 25. The provisions regulating internet usage in schools as was done in the USA need to be enshrined in Nigerian and South African laws. Obviously, the two countries are not yet parties to the African Union Convention on Cyber Security and Personal Data Protection 2014. Becoming parties can help both countries in reviewing their legislation.

(2) For adequate implementation and enforcement of legislation, it is crucial for both Nigeria and South Africa to mobilise, allocate and utilise public resources, policies and programmes aimed at fully upholding children's rights in the digital environment, enhancing digital inclusion to address the growing impact of the digital world on children's lives, and promoting equal access to affordable services and connectivity. This is in line with paragraph 21 of General Comment 25 which states the obligation of state parties to undertake 'all appropriate measures', including the duty to ensure that laws and policies are established to facilitate resource mobilisation, budget allocation, and expenditure for the realisation of children's rights, and that relevant data and information on children are gathered and disseminated to support the implementation of appropriate legislation, programmes, policies, and budgets aimed at advancing children's rights.[143]

(3) The Nigerian and South African governments should raise public awareness on the importance of children's digital rights and online safety in collaboration with businesses and civil society organisations. In this way, children should be educated on online safety techniques to protect themselves and their personal data in the digital space.[144] This includes providing parents, guardians, teachers and children with appropriate information on child online safety considering their different ages and evolving capacities. The use of local languages and braille is also encouraged for children with disabilities.[145]

13 Conclusion

The analysis in this article has illustrated that children stand to benefit highly from participating online but, at the same time, are exposed to many risks. The article also indicates that safeguarding children's rights to privacy online is not yet explicitly enshrined in both Nigerian and South African children's rights laws, while the general laws do not contain comprehensive provisions. As rightly asserted by Livingstone and others, digital media are no longer luxuries; they are expeditiously becoming essential to modern life globally.[146] Due to the challenge of understanding and managing the digital innovations, governments worldwide, together with organisations dedicated to children's welfare, are advocating a principled, unified and evidence-based framework to acknowledge and uphold the best interests and rights of children.[147] By this, the fulfilment to children of the

143 UN CRC Committee General Comment 19 (2016) on public budgeting for the realisation of children's rights para 21.

144 T Iyoha-Osagie & OI George 'The right to online data protection of children: Examining the adequacy of the legal frameworks in Nigeria' (2019) 3 *ABUAD Private and Business Law Journal* 82-109.

145 UNICEF 'Child safety online: Global challenges and strategies technical report (UNICEF 2012) 78-79, www. unicef-irc.org/publications/652-child-safety-online-globalchallenges-and-strategies-technical-report.html (accessed 13 April 2024).

146 Livingstone and others (n 15).

147 As above.

ethical obligations in this respect is a matter of practical necessity.[148] Therefore, the governments of South Africa and Nigeria must rise up to the task of not only affording children adequate opportunities and means for participation online, but also providing comprehensive legal frameworks for children's privacy safeguard from risks such as cyber-aggression, technology-facilitated harm, online exploitation and child sexual abuse, a recommendation of the CRC Committee's General Comment 25 and practised in the USA.

148 As above.