# PRIORITISING CHILD RIGHTS PROTECTION IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE: ASSESSMENT OF THE GLITCHES AND GAINS IN NIGERIA*

**Abstract**
*Artificial intelligence (AI) drives a lot of activities in many sectors and structures in our society presently. Children are not shut out in the context of this advancement of Artificial Intelligence, thereby bringing to the fore, the concern of child rights protection in this digital age. Though, artificial intelligence will in many ways provide prospects and advantages to children, it on the other hand poses a lot of risks to their rights, development and well-being, especially in cases of AI interactions devoid of parental guidance and age-inappropriate applications and programs. This work therefore appraises child rights protection in the context of artificial intelligence with a view to accentuating the prospects and challenges of Artificial intelligence on Childs rights and well-being. The article adopts a doctrinal research methodology, relying on primary and secondary legal materials, including relevant international and regional human rights instruments, national legislation, judicial decisions, regulatory frameworks and scholarly literature. The study discovered and concluded that AI technologies have the likelihood of exposing children to dangerous or injurious content, excessive data collection that threaten their privacy rights and other forms of exploitation which raise fundamental questions concerning the extent to which existing child-rights laws are capable of regulating emerging AI technologies and providing effective remedies where children's rights are violated. It is recommended inter alia that Before AI systems are deployed, mandatory child-rights impact assessments should evaluate their effects on children's well-being and data-protection laws, and AI safeguards should be strengthened through privacy-by-design, safety testing, accountability measures and criminalisation of AI-generated child sexual abuse material.*

**Keywords:** Artificial Intelligence, Child Development, Children, Child Rights, Technology.

## 1. Introduction

We live in a digital world, where children's interaction with technological devices in many facets of their lives, such as in education, entertainment, acquisition of skills and obtaining of information is inevitable, thereby making special and effective attention to child's rights imperative in order to checkmate violations. This is because, unlike adults, children are immature and need adequate protection of their rights for the realisation of their full potentials. Artificial Intelligence (AI) has become one of the most influential technological developments of the twenty-first century, transforming the way individuals live, work, communicate, and access essential services. Although AI as a field of study dates back to the 1950s, recent advances in machine learning, deep learning, cloud computing, and data analytics have accelerated its integration into everyday life.

Today's children encounter a wide range of artificial intelligence agents, each built for different purposes and with varying levels of sophistication. Many of these systems are voiced based like Alexa and Siri, or chat based like Chat GPT & Meta AI, and produce replies in a conversational manner. Researchers studying children's development are deeply interested in how children actually engage with these agents in everyday contexts. Observing how children talk with AI offers insights not only into their usage patterns but also their interpretations and expectations of these systems.[1]

The use of artificial intelligence (AI) in education has enabled personalized learning, revolutionizing the way students learn. For instance, platforms such as uLesson, which uses AI-driven adaptive learning algorithms to deliver personalised video lessons and quizzes aligned with the Nigerian curriculum, have gained substantial traction.

Nigeria has one of the highest rates of social media engagement among young people in Africa. The Data Reportal Digital 2024 Nigeria report indicated that 31.6 million Nigerians aged 13 and above use social media, with WhatsApp, Facebook, TikTok, and Instagram being the most popular platforms.[2] A study in Enugu State showed that 67 per cent of primary school children with access to a smartphone had used a voice assistant. Many treated it like a companion, even when it failed to understand local languages[3] The available data indicate that Nigerian children are increasingly interacting with artificial intelligence through multiple channels which also suggests the significant gaps in children's AI literacy, the uneven distribution of AI benefits, and heightened exposure to digital harms among marginalised populations.

***By Chinazor Queen UMEOBIKA, PhD,** Reader and Head, Department of Private and Property Law, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. cq.umeobika.@unizik.edu.ng, queencumeobika@gmail.com; Tel: 08035018582; and

***Linda Amarachi OTI-ONYEMA, PhD,** Lecturer, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria, Email: la.oti-onyema@unizik.edu.ng; amyonyema1985@gmail.com.

[1] Y Xu and K He, *Growing up with Artificial Intelligence: Implications for Child Development* (Cambridge University Press 2026).

[2] Datareportal, Digital 2024: Nigeria (Datareportal 2024) <Https://Datareportal.Com/Reports/Digital-2024-Nigeria> Accessed 16 June, 2026.

[3] C Ugwu, I Eze and B Okafor, 'Smartphone Use Among Primary School Children in Enugu State: Patterns and Implications' *International Journal of Child Development and Technology* (2023) 10, 112–118.

Realising the need to secure the protection of the child from the negative effects of AI, certain legal framework has been established both nationally and internationally such as Constitution of the Federal Republic of Nigeria[4], Child Rights Act[5], Nigeria Data Protection Act[6], Cybercrimes (Prohibition, Prevention, etc.) Act[7], Nigerian Communications Act[8], the NCC Internet Code of Practice[9] 2026, UN Convention on the Rights of the Child (CRC), African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).

Despite the above legal regimes, AI is deployed in education, entertainment, and social platforms without systematic consideration of the best interests of the child, without meaningful participation of children in design or oversight, and without enforceable obligations on developers and operators to protect children from algorithmic harm.[10] There is inadequate prioritisation of child's rights in AI governance and Nigeria's legal framework reflects this neglect. Historically, child rights have been subjected to numerous violations across the world. Children have been exploited through child labour, recruited into armed conflicts, trafficked for commercial sexual exploitation, denied access to education and healthcare, and exposed to conditions that threaten their health, safety, and overall development daily. For much of legal history, children were treated as objects of adult authority rather than as autonomous bearers of entitlements.[11] This study, therefore, becomes very important to examine the implications of Artificial Intelligence (AI) for the protection of children's rights by assessing both the opportunities and the challenges associated with the increasing deployment of AI technologies.

## 2. Conceptual Clarifications

### Artificial Intelligence

According to John McCarthy, known as the 'Father of Artificial Intelligence,' AI is 'the science and engineering of making intelligent machines, especially computer programs that can perform tasks that, if performed by humans, require intelligence'.[12] Artificial intelligence (AI) traditionally refers to an artificial creation of human-like intelligence that can learn, reason, plan, perceive, or process natural language.[13] It is conceived as computer systems that are similar to the human mind in a certain sense, though a computer and a human mind cannot be identical in all aspects.[14] Artificial intelligence is a designed structure for logical, exploratory, pattern recognition, inference making, and experiential learning[15]. In general, the term 'artificial intelligence' is a branch of information technology that focuses on creating tools and programmes that can imitate intelligent behaviour such as sensing, learning and predicting.[16] Rather than simply following fixed instructions, AI systems can analyze large amounts of data, identify relationships, and improve their performance over time through techniques such as machine learning and deep learning.

### Digital Childhood

Digital childhood denotes the condition in which children's development, play, learning, and social relationships are pervasively mediated by digital technologies from their earliest years.[17] Sociologists of childhood emphasise that childhood is a social construction that varies across time and culture.[18] The new sociology of childhood insists that children are active interpreters of their worlds, not passive recipients of socialisation[19]. The digital turn of socialisation represents one of the most profound restructurings of that construction, embedding children in an ecosystem of connected toys, tablets, apps, and smart environments. Digital media though offering new avenues for communication, creativity and participation[20], it also turns children's everyday activities into measurable data streams. Lupton and Williamson coined the term 'datafied child' to capture how feeding, sleeping, movement, learning, and emotion are increasingly

[4] 1999
[5] 2003
[6] 2023 (NDPA)
[7] 2015
[8] 2003
[9] 2026
[10] UN Committee on the Rights of the Child, 'General Comment No 25 (2021) On Children's Rights in Relation to the Digital Environment' (2021) UN Doc CRC/C/GC/25, Paras 2–10.
[11] D Archard, *Children: Rights and Childhood* (2nd Edn, Routledge 2004).
[12] R Rodrigue, 'Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities' *Journal of Responsible Technology* (2000) 4(3).
[13] 'Artificial Intelligence' (Wikipedia) <Https://En.Wikipedia.Org/Wiki/Artificial_Intelligence > Accessed 18 May 2026.
[14] P Wang, 'On Defining Artificial Intelligence' *Journal of Artificial General Intelligence* (2019) 10(2), 1–37.
[15] J Mccarthy, 'What Is Artificial Intelligence' (2004) <Http://Www-Formal.Stanford.Edu/Jmc/Whatisai.Html > Accessed 18 May 2026
[16] A Jain, 'Artificial Intelligence and Child Rights: An Analysis' *International Journal of Legal Developments and Allied Issues* (2022) 8(3) < Https://Thelawbrigade.Com/ > Accessed 18 May 2026
[17] D Holloway, L Green and S Livingstone, *Zero to Eight: Young Children and Their Internet Use* (EU Kids Online 2013).
[18] WA Corsaro, *The Sociology of Childhood* (5th Edn, SAGE 2018).
[19] A James and A Prout (Eds), *Constructing and Reconstructing Childhood* (2nd Edn, Falmer Press 1997).
[20] S Livingstone, *Children and the Internet: Great Expectations, Challenging Realities* (Polity 2009).

tracked, digitised, and fed into commercial and institutional databases.[21] Digital childhood is therefore a datafied childhood, where the child is constituted through digital traces before they can knowingly consent.

**Child Rights**

Generally, in law, who a child is, is determined by age of the person under consideration. The term usually refers to anyone below the age of majority but has been used interchangeably with terms such as infant, minor, juvenile amongst others.[22] In Nigeria, the child is defined as 'a person under the age of eighteen years,' while 'age of majority' is defined as the age at which a person attains eighteen years under the CRA. This CRA's definition of a child accords with the internationally accepted definition of a child. Generally, under international law, there appears a consensus that a child is a person under the age of 18years. *Article 1* of the Convention on the Rights of the Child, (CRC) in defining a child stated that: 'For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier. The definition of a child under the Convention on the Rights of the Child (CRC) seeks to achieve a measure of uniformity among State Parties, while simultaneously allowing for the recognition of diverse national age thresholds. Nonetheless, although the Convention permits States to set a lower age limit, it does not allow the extension of childhood beyond eighteen years.[23] Child Rights are a specialized subset of human rights specifically allocated to individuals under the age of eighteen because of their unique developmental stage, vulnerability, and physical and mental immaturity.

**Child Rights Protection**

Child Rights protection refers to the prevention of, and response to abuse, neglect, exploitation, violence, and all forms of harm against children. It encompasses legal, institutional, and social frameworks designed to safeguard children from physical, emotional, psychological, and sexual abuse/ harm while promoting their welfare and best interests. Child rights protection is rooted in the recognition that children, by reason of their age and developmental stage, require special legal, social, and institutional safeguards to ensure their continued survival, development, and overall well-being. Unlike adults, children possess limited capacity to protect their own interests and are therefore entitled to enhanced protection under both domestic and international law. Child rights protection is the creation of an environment in which the child can develop the capacity for autonomous action while being shielded from harms that would destroy or undermine that capacity.

**3. Legal and Institutional Framework for Prioritizing Child Rights Protection in the Digital Space**

**United Nations Convention on Rights of the Child (UNCRC)**

The UN Convention on the Rights of the Child (UNCRC) is the main international legal framework for protecting children's rights. It is the most complete statement of children's rights ever produced and is the most ratified international human rights treaty in history. Nigeria ratified it in 1991, and it was domesticated through the Child Rights Act 2003. The UNCRC has been steadily developed to address issues regarding child rights especially in the ever-evolving digital world. In 2021, the UN Committee on the Rights of the Child officially launched their new General Comment No. 25 on Children's rights in relation to the digital environment.[24] The adoption of this General Comment signals the first time that children's digital experiences are mentioned within the UNCRC.

Principles of the convention that are relevant to AI include:

*Article 2- Non-discrimination*: Article 2 requires states to respect and ensure the rights in the Convention to every child without discrimination of any kind. General Comment No. 25 explicitly provides that states must 'take measures to prevent discrimination in the digital environment, including by addressing algorithmic bias.'[25] For instance, algorithm bias is evident when an AI learning platform recommends academic tracks based on historical data which may steer girls away from science subjects or place children from poorer backgrounds into lower-ability groups. This transforms non-discrimination from a passive obligation and challenges AI systems that produce discriminatory outcomes to audit and correct their datasets.

*Article 3- Best Interest of a Child*: Article 3(1) obliges that 'in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best

[21] D Lupton and B Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' *New Media & Society* (2017) 19(5), 780–794.

[22] LA Oti-Onyema, (2018). Right of the Child to Land Acquisition in Nigeria: The Capacity Challenge. *ABUAD Private and Business Law Journal*, *2*(1), 149-173.

[23] C. Q. Umeobika, & L. A. Oti-Onyema, (2025), 'Incongruity in Definitions of a Child: Implications for Criminal Responsibility' In Nigeria. *Law And Social Justice Review*, *6*(2).

[24] UN Committee on the Rights of the Child, 'General Comment No 25 (2021) On Children's Rights in Relation to the Digital Environment' (2021) UN Doc CRC/C/GC/25

[25] Ibid Para 10

interests of the child shall be a primary consideration'. General Comment No. 25 clarifies that states must ensure that the best interests' principle is integrated into all legislation, policies, and practices relevant to the digital environment, and that business enterprise, including technology companies, must incorporate it into the design of their products and services.[26]

*Article 13 – Freedom of Expression***:** Article 13 protects the child's right to seek, receive, and impart information and ideas of all kinds. With the increasing use of AI systems as search engines, AI systems are now the gatekeepers of information. When an AI system filters, demotes, or promotes certain content, it directly affects this right. States must ensure that children can access diverse information through digital platforms and that algorithmic curation does not narrow their information environment in ways that harm their development or participation in cultural and public life.[27]

*Article 16- Privacy***:** Article 16 prohibits arbitrary or unlawful interference with the child's privacy, family, home, or correspondence. In the digital context, this provision ensures the child's right to data protection and limits on surveillance.[28] AI systems that collect, aggregate, and profile children's personal data engage this right directly. The Committee has stressed that states must prohibit the profiling or targeting of children for commercial purposes and require data protection by design and by default.[29]

*Article 17- Access to Appropriate Information:* Article 17 specifically obliges states to encourage the production and dissemination of information of social and cultural benefit to the child and to protect children from material injurious to their well-being. This article is particularly relevant to AI-driven content recommendation. States must encourage platforms to develop and use algorithms that prioritise diverse, educational, and age-appropriate content, rather than optimising solely for engagement.[30]

*Article 19- Protection from All Forms of Violence:* Article 19 obligates states to take all appropriate measures to protect the child from all forms of physical or mental violence, injury, or abuse, including while in the care of parents or any other person who has care of the child. This obligation is extended by General Comment No. 25 to the digital environment, explicitly listing online forms of violence: cyberbullying, exposure to violent or graphic content, and grooming.[31] Generative AI can create synthetic child sexual abuse material; algorithmic systems can facilitate grooming by recommending adult strangers to children or failing to detect predatory behaviour.[32]

*Article 34- Sexual Exploitation:* Article 34 encourages states to protect children from all forms of sexual exploitation and abuse, including in prostitution and pornography. The UN Committee has stated that this includes the production, distribution, and possession of child sexual abuse material in digital forms, including computer-generated or AI-generated imagery that realistically depicts children.[33] The proliferation of AI generated images and deep fakes with childlike images have become a growing concern and the need to regulate such generative AI systems is urgent.

*Articles 28 and 29- Education***:** Articles 28 and 29 guarantee the right to education and set out its aims, including the development of the child's personality, talents, and mental and physical abilities to their fullest potential. General Comment No. 25 insists that digital education technologies must support, not replace, teacher-led instruction, and that states must regulate Edtech providers to ensure that their AI systems do not undermine the goals of education through commercial data extraction or narrow pedagogical models.[34]

States must enact legislation requiring technology companies to conduct child rights impact assessments, to embed the best interest principle into the design of AI systems, to be transparent about how algorithms affect children, and to provide accessible remedies when rights are violated.[35]

**Nigerian Law**

**Constitution of the Federal Republic of Nigeria 1999:** The first legal instrument to be considered is the Constitution of the Federal Republic of Nigeria 1999 (as amended), which constitutes the *Grundnorm* and the supreme law of the Nigerian legal order. By virtue of its constitutional supremacy, all other laws, policies and regulatory measures derive

[26] Ibid Para 10
[27] Ibid Para 53.
[28] Ibid Para 67.
[29] Ibid Para 71.
[30] Ibid Para 55.
[31] Ibid Para 82.
[32] Ibid Paras 84–85.
[33] Ibid Para 86.
[34] Ibid Paras 100–101.
[35] Ibid Paras 34–39.

their validity from, and must conform to, the Constitution.[36] Although the Constitution does not contain an express and comprehensive framework specifically addressing the rights of the child in the digital environment, it guarantees a number of fundamental rights that are directly relevant to the protection of children online.

In particular, rights corresponding to several protections recognised under the Convention on the Rights of the Child (CRC) are reflected, either expressly or by necessary implication, within the constitutional framework. These include the right to dignity of the human person[37], the right to privacy and family life[38], and the freedom of expression[39], amongst other fundamental rights. Accordingly, while the Constitution does not expressly articulate a distinct category of 'digital rights' or 'children's digital rights,' its existing fundamental rights provisions provide a constitutional basis for addressing aspects of children's rights in the digital environment.

The absence of provisions specifically tailored to the peculiar vulnerabilities and circumstances of children in the digital environment creates a degree of normative and regulatory limitation. The constitutional provisions must therefore be considered alongside Nigeria's statutory and international legal obligations relating to child protection and digital rights in determining the extent to which children are adequately protected in the digital sphere.

**Child's Rights Act 2003:** The provisions of the CRA to a great extent replicates the provisions of the CRC on the rights of the child. Although enacted before the emergence of contemporary AI technologies, the CRA provides principles capable of guiding the development and deployment of AI systems in ways that prioritise children's rights, welfare and development. Central to the CRA is the best interests of the child principle. Section 1 provides that, in every action concerning a child, whether undertaken by an individual, public or private body, institution or court of law, the best interests of the child shall be of paramount consideration. This provides a particularly important normative standard in the context of AI. AI systems are increasingly capable of influencing decisions and experiences that affect children, including education, access to information, content recommendation and digital interaction. The best interests principle therefore provides a basis for requiring that the potential impact of such systems on children's welfare, development, dignity, privacy and safety be considered before and during their deployment.

The CRA further recognises rights that are directly implicated by the increasing use of AI and digital technologies such as the child's right to privacy, family life, education, development, welfare, protections against exploitation and harmful practices, as well as provisions concerning the child's education, development and welfare. These protections have both defensive and enabling dimensions in the AI context. On the one hand, they provide a basis for protecting children from AI-enabled harms, including exposure to harmful content, manipulation, exploitation and other forms of digital abuse. On the other hand, they support the responsible use of AI to advance children's educational opportunities and development.

**Nigeria Data Protection Act 2023:** The Act adopts a rights-based approach to data protection by recognising the interests and rights of data subjects and imposing obligations on data controllers and processors. Of particular relevance to children is section 31 of the NDPA, which establishes specific safeguards in relation to the processing of personal data of a child. The provision recognises the particular vulnerability of children and places additional requirements on the processing of their personal data. This is important in the AI context because children may be unable to fully understand the implications of providing personal information to AI-powered platforms or the extent to which such information may subsequently be analysed, profiled or used for other purposes. The protection of children's data under the NDPA is further reinforced by the Act's general principles governing the processing of personal data. *Section 24* requires personal data to be processed in a manner that is lawful, fair and transparent and for specified, explicit and legitimate purposes. The NDPA also provides data subjects with important rights, including rights relating to access, rectification, erasure and objection to certain forms of processing. These rights can contribute to the protection of children whose personal information is processed by AI-driven platforms.

**Cybercrimes (Prohibition, Prevention, etc.) Act 2015:** The Act primarily seeks to prevent, prohibit and prosecute offences committed through computer systems and networks. Although it was not enacted specifically to regulate artificial intelligence (AI) or to establish a comprehensive framework for children's digital rights, several of its provisions are relevant to protecting children from technology-facilitated exploitation and abuse. Of particular relevance is section 23, which criminalises cyberstalking and other forms of persistent online harassment and communication that cause fear, emotional distress or apprehension. This provision assumes greater significance in an AI-driven environment, where automated systems can facilitate the creation, dissemination and amplification of harmful communications and content

[36] Section 1
[37] Section 34
[38] Section 37
[39] Section 39

at considerable speed and scale. AI-generated material may also be used to impersonate, harass, threaten or otherwise target children. The Cybercrimes Act therefore provides a criminal-law mechanism through which certain forms of AI-enabled or AI-assisted abuse may potentially be addressed.

**EU AI Act:**[40] The AI Act is the first AI regulation which recognises children's rights in the digital environment as set out in General Comment No. 25 to the UN Convention on the Rights of the Child.[41] The Act contains several important safeguards for children. Most significantly, Recital 48 expressly recognises children's specific rights under Article 24 of the EU Charter of Fundamental Rights and the UN Convention on the Rights of the Child, requiring their vulnerabilities and protection needs to be considered in AI governance. A major gain is the Act's treatment of education-related AI systems. Article 6(2), read with Annex III, point 3, classifies certain AI systems used in education and vocational training as high-risk, particularly where they determine access or admission to educational institutions, assign students to institutions or programmes, evaluate learning outcomes, assess educational levels, or otherwise influence educational opportunities. This provides heightened protection where AI decisions could significantly affect a child's educational trajectory and future opportunities.[42]

The Act also addresses the exploitation of children's age-related vulnerability. Article 5(1)(b) prohibits AI systems that deploy manipulative or deceptive techniques that materially distort a person's behaviour where significant harm is likely to result, while Article 5(1)(b) also covers systems exploiting vulnerabilities due to age or other specific characteristics where significant harm is likely. This is particularly relevant to AI systems capable of influencing children's behaviour, including personalised or anthropomorphic systems.[43] In addition, Article 27 requires certain deployers of high-risk AI systems to conduct a fundamental-rights impact assessment, providing an opportunity to identify and mitigate potential effects on fundamental rights before deployment. This is significant for children where high-risk AI is deployed in settings such as education or other areas capable of substantially affecting their rights.

Taken together, these provisions represent important gains in child-rights protection because the EU AI Act moves beyond general data protection by recognising children's vulnerability, subjecting specified educational AI systems to heightened regulation, prohibiting certain forms of manipulation and requiring fundamental-rights assessments. Nevertheless, the Act remains primarily a general AI regulatory framework rather than a comprehensive child-rights instrument, leaving some risks associated with children's everyday interaction with AI outside the strongest regulatory categories. Certain limitations emerge within the Act in relation to children's needs and challenges. One gap is around responding to the full spectrum of harms caused by deepfake technology.

For context, the surge of free and easily accessible generative AI tools in recent years has led to a rise in minors creating and sharing non-consensual, manipulated imagery of each other as a tool for bullying and shaming. This raises concerns about the extent to which the EU AI Act adequately addresses the broader child-rights implications of deepfakes used for bullying, humiliation or exploitation, particularly their potential effects on children's emotional well-being, social relationships, dignity and educational experiences. Although the Act contains provisions addressing certain harmful AI practices and, more recently, has been strengthened to address non-consensual intimate material and child sexual abuse material, the broader and non-sexualised harms arising from deepfake-enabled bullying and humiliation are less expressly addressed within the AI Act. This leaves an important question as to whether the risk-based framework sufficiently captures the cumulative and context-specific harms that AI-generated manipulated content can inflict on children.

**United States' Children's Online Privacy Protection Act:**[44] This landmark regulation provides parents greater control and insights over what data websites can collect from their children and ensures children can continue navigating the Internet safely and securely. The provisions of the law apply to any operator of a website or an online service directed to children and any operator that has actual knowledge that it is collecting or maintaining personal information from a child.[45] Operators are generally required to notify[46] and obtain verifiable parental consent before collecting, using or disclosing a child's personal information and before making material changes to previously consented data practices. Parents must also be given the option to consent to the collection and use of their child's information without consenting to its disclosure to third parties. Verifiable consent may be obtained through signed consent forms, online payment mechanisms, telephone or video verification, or government-issued identification.[47]

---

[40] (Regulation (EU) 2024/1689)
[41] Andra Siibak & Giovanna Mascheroni Digital Futures: Prioritising Children's Rights in the World of AI, <https://link.springer.com/chapter/10.1007/978-981-95-8922-7_5>, accessed on 10/10/2026
[42] N Kurian, 'EU AI Act: How Well Does it Protect Children and Young People?', <https://www.lcfi.ac.uk/news-events/blog/post/eu-ai-act-how-well-does-it-protect-children-and-young-people,> , accessed on 10/10/2026
[43] *Ibid.*
[44] 1998 (COPPA)
[45] 16 C.F.R. § 312.3
[46] 16 C.F.R. § 312.4
[47] Section 312.5,

However, parental consent is not required in certain limited circumstances, including where information is collected solely to notify or communicate with parents, respond to a child's one-time or limited requests, protect a child's safety, or support internal website operations. Exceptions also apply where information is collected to comply with legal obligations, respond to lawful requests, protect website security, or assist law-enforcement investigations relating to public safety. These exceptions are generally subject to restrictions on further use, disclosure and retention of the child's information.[48] The Act prohibits against conditioning a child's participation in a game or website service, prize winnings, or any other activity on the child disclosing more personal information than is necessary for the child's participation in such activities.[49]

Confidentiality, Security, and Integrity of Collected Personal Information are the hallmark of the Act. Thus, operators must undertake all reasonable efforts to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected from children. Such measures should specifically be extended towards ensuring that such personal information is only shared with service providers and third parties with similar adequate measures to protect such information's confidentiality, security, and integrity. The operator must also seek written assurance from such third parties guaranteeing their maintenance and implementation of the security measures.[50]

An operator of the website has a duty to retain all personal information collected from a child for as long as reasonably necessary to fulfil the purpose for the collection and in a context consented to by the parent. The operator must delete such information via reliable measures whenever requested by the parent under the provisions of these regulations.[51] A parent has the right to request a review of any and all personal information a website may have collected on a child. The operator of such a website is obligated to provide the parent with such information as requested upon verifying and ensuring that the request is made from the parent of the child via appropriate technological measures.[52] Similarly, an operator may choose to terminate any services provided to a child whose parents have refused to permit the collection of their child's personal information and has requested the deletion of the child's personal information.[53]

However, neither an operator nor the operator's agent may be held liable under any federal or state law for any disclosures they may choose to make in good faith within procedures while responding to a request for disclosure of personal information per the requirements. Non-compliance with the Children's Online Privacy Protection Act (COPPA) may attract substantial financial penalties and court-ordered remedies. Under the Act and its implementing regulations, operators of websites and online services that unlawfully collect, use, or disclose children's personal information may face enforcement action by the Federal Trade Commission (FTC) and other authorised agencies.[54] In *United States v Microsoft Corporation*, it was held that Microsoft will pay $20 million to settle FTC charges that it violated COPPA by collecting personal information from children who signed up to its Xbox gaming system without notifying their parents or obtaining their parents' consent, and by illegally retaining children's personal information.[55]

**Comparative Analysis**

Although the Children's Online Privacy Protection Act (COPPA) is primarily concerned with protecting children's online privacy, rather than addressing the broader spectrum of child-protection concerns, such as exploitation and other AI-related harms, encompassed by the EU AI Act which addresses a wider range of AI-related risks, it remains relevant to this discourse. COPPA strengthens parental oversight of children's digital interactions. It generally requires verifiable parental consent before covered operators collect personal information from children under thirteen, subject to exceptions.

Furthermore, the proposed Kids Internet and Digital Safety (KIDS) Act[56] represents another significant legislative initiative aimed at strengthening children's online safety in the United States. Kids Internet and Digital Safety (KIDS) Act. The KIDS Act consolidates a variety of legislative proposals aimed at protecting children and teens online including the Kids Online Safety Act (KOSA), which would require online platforms to adopt default safeguards for minors. The Act is a package intended to protect minors from various dangers presented by online platforms such as social media and AI chatbots. The legislation includes measures regarding age verification, minors' access to sexually explicit material,

[48] Section 312.5(c)
[49] Section 312.7
[50] Section 312.8
[51] Section 312.10
[52] Section 312.6(a)(1)
[53] 312.6(a)(2)
[54] A Baig & A Hasan, 'What is COPPA (Children Online Privacy Protection Act)?' < https://securiti.ai/children-online-privacy-protection-act-of-1998-overview/>, accessed on 10/10/2026
[55] *United States v Microsoft Corporation*, No. 2:23-cv-00836 (W.D. Wash. June 12, 2023)
[56] H.R. 7757

limits on 'design features that result in compulsive usage,' and tools enabling parents to view the total time their child spends on a platform.[57]

These regulatory developments offer valuable lessons for Nigeria, particularly in developing a comprehensive child-centred legal framework that addresses not only data privacy but also the risks of exploitation, harmful algorithmic practices and other threats arising from children's interaction with artificial intelligence. Nigeria should therefore draw from these comparative experiences in strengthening its legal and institutional mechanisms for protecting children in the AI era.

## 4. Gains and Opportunities of AI for Children

It would be analytically incomplete and ultimately misleading to approach the subject of AI and child rights solely through the prism of risk. Artificial intelligence, when responsibly developed and equitably deployed, carries genuine and substantial potential to advance the rights and wellbeing of children, particularly those in regions such as Nigeria and Sub-Saharan Africa where structural deficits in education, healthcare, and child protection remain severe. This section therefore examines the opportunities and gains of AI for children's rights.

### Education and Learning

AI can enhance education through personalised learning, adaptive content and immediate feedback tailored to individual children's needs. These capabilities are particularly valuable in Nigeria, where teacher shortages, overcrowded classrooms and inadequate educational funding limit access to quality education.[58] A World Bank-supported study in Edo State reportedly found that generative AI tutoring improved students' English-language performance within six weeks.[59] Similarly, Nigeria's EdTech company uLesson uses digital learning tools and analytics to support students, including those in underserved communities.[60] These applications demonstrate AI's potential to supplement traditional teaching and widen access to learning opportunities. From a rights-based perspective, AI-assisted education may help advance the right to education by reaching children underserved by conventional educational systems. However, its effectiveness depends on affordability, reliable infrastructure, educational quality and appropriate safeguards.

### Healthcare and Well-being

AI offers opportunities to improve children's health through disease detection, predictive health analytics and early developmental screening. These applications may support the identification of illnesses and developmental conditions, enabling earlier intervention, particularly in communities with limited access to specialist healthcare.[61] AI has also been applied to child-protection services. For instance, Pennsylvania's Allegheny Family Screening Tool (AFST) analyses administrative data to assist child-welfare caseworkers in assessing reports of possible maltreatment.[62] Although predictive systems raise concerns about bias, privacy and accountability, carefully supervised applications may help prioritise cases requiring urgent attention. AI should, however, support rather than replace professional judgment and child-centred assessment.

### Inclusion and Accessibility for Children with Disabilities

AI-powered assistive technologies can improve access to education, communication and social participation for children with disabilities. Despite the global need for assistive products, access remains unequal, particularly in low- and middle-income countries.[63] Speech recognition, text-to-speech, automated captioning and image-description tools can help children with visual, hearing, motor or learning impairments participate more fully in educational activities. Applications such as Microsoft's Seeing AI, for instance, describe visual information for people with visual impairments.[64] These technologies can advance the principles of non-discrimination under Article 2 of the UNCRC and the protection of children with disabilities under Article 23. In Nigeria and other African countries, affordable and accessible AI tools could improve educational inclusion and participation, provided that infrastructure, cost and accessibility barriers are addressed.

---

[57]https://www.cnbc.com/make-it/2026/07/02/a-major-online-safety-bill-for-kids-just-passed-the-housewhat-parents-need-to-know.html

[58] LK Nhan, 'The Role of AI In Enhancing Personalized Learning' <Https://Dergipark.Org.Tr/En/Download/Article-File/4488257> Accessed 1 July 2026.

[59] Supra, Note 2.

[60] Supra, Note 1.

[61] T Maruta, 'The Role of Artificial Intelligence in Diagnostics: A New Frontier for Laboratory Medicine in Africa' *African Journal of Laboratory Medicine* <Https://Ajlmonline.Org/Index.Php/Ajlm/Article/View/2952/3262> Accessed 1 July 2026.

[62]*Ibid.*

[63] UNICEF, 'Global Report on Assistive Technology, A WHO-UNICEF Joint Report. <Https://Www.Unicef.Org/Reports/Global-Report-Assistive-Technology> Accessed July 1st, 2026.

[64]N Kukushkina, 'How AI Systems Can Support People with Disabilities' Digitalmara <Https://Digitalmara.Com/Blog/How-Ai-Systems-Can-Support-People-With-Disabilities/> Accessed 1 July 2026.

**Language Translation and Accessibility Tools**
AI-powered translation and speech technologies can reduce language barriers that prevent children from fully benefiting from education. Tools such as Google Translate, Microsoft Translator and Meta's No Language Left Behind model facilitate the translation of educational content into multiple languages, including some African languages.[65] Multilingual voice interfaces and speech-recognition systems may further enable children to access educational resources in their preferred languages, including those who have not yet developed strong literacy skills.[66] These technologies can make learning more comprehensible and culturally relevant, thereby supporting meaningful access to education. Their effectiveness, however, depends on the accuracy of translation, adequate representation of African languages in training data and the availability of appropriate digital infrastructure.

**AI in Child Protection and Welfare Systems**
AI offers opportunities to strengthen child protection by analysing large datasets to identify children at risk, prioritise limited resources and support informed decisions in child-welfare proceedings.[67] Predictive analytics can combine social service records, health information, school attendance and previous maltreatment reports to flag cases requiring further investigation. Similarly, AI-powered digital forensic tools can assist law enforcement in detecting and analysing child sexual abuse material (CSAM), enabling the examination of large volumes of digital evidence. However, these technologies should complement, rather than replace, professional judgment and must incorporate safeguards against bias, privacy violations and erroneous risk assessments.[68]

**5. Glitches, Risks, and Challenges of AI on Child's Rights**
Having analyzed the gains of AI in protecting children's rights in the preceding section, this section critically examines the bottlenecks posed by artificial intelligence on child's rights.

**Privacy and Data Exploitation**
Children's right to privacy under Article 16 of the UNCRC, as interpreted in General Comment No. 25, is threatened by AI systems that collect and analyse browsing habits, location, social interactions, educational performance and behavioural patterns. Such data may be commercialised without adequate transparency or meaningful parental involvement.[69] The gravity of this violation was authoritatively established in the United States in the landmark enforcement case of *FTC v Google LLC and YouTube LLC*[70] in which the Federal Trade Commission and the New York Attorney General secured a settlement of $170 million, the largest in the history of the Children's Online Privacy Protection Act (COPPA) against Google and YouTube for the unlawful collection of personal data from children under the age of thirteen without parental consent targeted at advertising. In Nigeria, the Nigeria Data Protection Act (NDPA) 2023 provides safeguards for children's personal data. Section 31 generally requires parental or guardian consent where consent is the basis for processing a child's data, subject to specified exceptions. However, the interaction between section 31(5), which addresses children aged 13 and above requesting electronic services, and section 65, which adopts the definition of a child under the Child Rights Act 2003, creates uncertainty requiring clarification. Furthermore, the absence of a comprehensive AI-specific child-protection framework leaves emerging risks, including automated profiling and AI-driven surveillance, insufficiently addressed by dedicated regulation.

**Exposure to Harmful Content: Deepfakes, Misinformation, and AI-Generated Child Sexual Abuse Material**
Generative AI has increased the ease with which users can produce deepfakes, misleading content and AI-generated child sexual abuse material (AIG-CSAM). The National Center for Missing and Exploited Children reported a 1,325% increase in Cyber Tipline reports involving generative AI between 2023 and 2024. It subsequently recorded more than 400,000 reports involving generative AI in 2025, although not all concerned AI-generated CSAM.[71] The legal and prosecutorial challenge posed by AIG-CSAM that does not depict identifiable real children remains threatening, producing what scholars have described as a fractured legal landscape.[72] In the case of *United States v David Tatum*,[73] n United States v

[65] A Adepetun, '55 African Languages to Benefit as Meta's AI Machine Translation Debuts' The Guardian Nigeria News <Https://Guardian.Ng/Technology/55-African-Languages-To-Benefit-As-Metas-Ai-Machine-Translation-Debuts/> Accessed 1 July 2026.
[66] *Ibid.*
[67] S Mark, 'The Role of AI And Big Data in Identifying At-Risk Children' Child Protection Global Network <Https://Cpgn.Org/Blogposts/The-Role-Of-Ai-And-Big-Data-In-Identifying-At-Risk-Children/> Accessed 1 July 2026
[68] *Ibid.*
[69] P Hartung, 'The Children's Rights-By-Design Standard for Data Use by Tech Companies' UNICEF <Https://Www.Unicef.Org/Innocenti/Media/1096/File/UNICEF-Global-Insight-Datagov-Data-Use-Brief-2020.Pdf> Accessed 1 July 2026.
[70] FTC V Google LLC and Youtube LLC (2019) 1:19-Cv-02642
[71] R Pfefferkorn, S Grossman and Sunny Liu, 'AI-Generated Child Sexual Abuse Material: Insights from Educators, Platforms, Law Enforcement, Legislators, and Victims' Stanford Digital Repository Https://Purl.Stanford.Edu/Mn692xc5736 Accessed 1 July 2026.
[72] EH Vaughan, 'NCMEC Releases New Data: 2024 In Numbers' National Center for Missing & Exploited Children Https://Www.Missingkids.Org/Blog/2025/Ncmec-Releases-New-Data-2024-In-Numbers Accessed 1 July 2026.
[73] *United States V. David Tatum* (2023) No.23-4710.

David Tatum, a child psychiatrist was convicted of offences involving child sexual abuse material, including sexually explicit images created by manipulating photographs of real minors using AI. This case illustrates both the ease with which AI can be weaponised against specific children known to the perpetrator.[74] In Nigeria, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended, provides a framework for addressing child pornography and related cyber offences. Nevertheless, the application of existing provisions to synthetic imagery, particularly material generated without reference to an identifiable child, requires careful legal examination. This uncertainty highlights the need for clearer legislation addressing AI-generated sexual abuse material and cross-border enforcement.

**Algorithmic Bias and Discrimination**

AI systems may reproduce existing social inequalities when trained on biased or unrepresentative data. The Dutch childcare-benefit scandal illustrates the consequences: an algorithmic system disproportionately targeted families with dual nationality and ethnic-minority backgrounds, contributing to wrongful benefit-recovery decisions affecting thousands of households. Amnesty International identified the scandal as a serious example of discriminatory algorithmic decision-making.[75] In education, AI tutoring and assessment systems trained predominantly on English-language datasets or educational experiences from high-income countries may perform poorly for children whose first language is not English or whose learning environments differ from those represented in the training data.[76] In Nigeria, such biases could disadvantage rural children, children learning in indigenous languages and children with diverse learning needs, thereby deepening existing educational inequalities.[77]

**Developmental and Psychological Risks**

AI also presents developmental and psychological risks, including excessive engagement with algorithmically curated content, emotional attachment to AI companions and continuous behavioural monitoring.[78] Recommendation systems designed to maximise engagement may expose children to distressing or emotionally manipulative material, potentially contributing to adverse mental-health outcomes. AI companions and chatbots that simulate friendship or romantic relationships raise additional concerns, particularly for children experiencing loneliness, bullying or emotional difficulties. Although these systems may provide short-term companionship, excessive dependence may interfere with healthy interpersonal relationships and social development. Appropriate safeguards, parental guidance and age-sensitive design are therefore essential.[79]

**Governance and Accountability Gaps**

AI development has advanced faster than many regulatory systems can effectively oversee it, creating accountability gaps that are particularly significant in Nigeria and Sub-Saharan Africa.[80] The European Union's AI Act, Regulation (EU) 2024/1689, establishes a risk-based regulatory framework. It prohibits specified harmful AI practices and imposes requirements on certain high-risk systems, including those used in education and decisions concerning access to essential public services. Its provisions address matters such as risk management, human oversight and non-discrimination.[81] However, its direct territorial application does not provide equivalent protection to children in Nigeria. Nigeria's NDPA 2023 empowers the Nigeria Data Protection Commission to enforce data-protection obligations and requires data-protection impact assessments where processing is likely to pose high risks to individuals' rights and freedoms. Nevertheless, the Act is not a comprehensive AI-specific child-protection statute.[82] Consequently, accountability for AI-related violations of children's rights depends substantially on existing data-protection, cybercrime and child-rights laws, whose combined application may leave regulatory and enforcement gaps.[83]

## 6. Conclusion and Recommendations

As AI systems are enjoying increased integration into the daily lives of children, the attendant risks have never been more poignant. Although existing regulatory frameworks are developing to be more inclusive and provide protection for

---

[74] FBI, 'Charlotte Child Pornography Case Shows 'Unsettling' Reach of AI Imagery — FBI'<Https://Www.Fbi.Gov/News/Stories/Charlotte-Child-Sexual-Abuse-Material-Case-Shows-Unsettling-Reach-Of-Ai-Generated-Imagery> Accessed July 1st, 2026.

[75] Amnesty International, 'Dutch Childcare Benefit Scandal an Urgent Wake-Up Call to Ban Racist Algorithms' <Https://Www.Amnesty.Org/En/Latest/News/2021/10/Xenophobic-Machines-Dutch-Child-Benefit-Scandal/> Accessed July 1st, 2026.

[76] UNICEF, 'How AI Can Have Negative Impacts on Children.' <Https://Www.Unicef.Ch/En/Current/News/2024-11-20/How-Ai-Can-Have-Negative-Impacts-Children> Accessed July 1st, 2026.

[77] *Ibid.*

[78] *Ibid.*

[79] *Ibid.*

[80] UNICEF, 'Policy Guidance On AI For Children' <Https://Www.Unicef.Org/Innocenti/Media/1341/File/UNICEF-Global-Insight-Policy-Guidance-AI-Children-2.0-2021.Pdf> Accessed July 1st, 2026.

[81] European Union,, 'AI Act: Shaping Europe's Digital Future'<Https://Digital-Strategy.Ec.Europa.Eu/En/Policies/Regulatory-Framework-Ai> Accessed July 1st, 2026.

[82] L Jumoke, C Okolie and S Ngwi, 'AI Watch: Global Regulatory Tracker - Nigeria' White & Case LLP Https://Www.Whitecase.Com/Insight-Our-Thinking/Ai-Watch-Global-Regulatory-Tracker-Nigeria Accessed 1 July 2026.

[83] *Ibid.*

children in the digital environment particularly with their use of AI systems, more needs to be done. There is a need to review existing AI regulatory frameworks to offer adequate protection for the specific needs and vulnerabilities of children. While the new data protection law is a step forward, it still does not cover the way algorithms make decisions about children or build profiles on them. Internationally, there are clear standards for protecting children in the digital world, but they have not been turned into working rules in Nigeria. The goal is not to stop progress but to make sure progress does not come at the expense of children's safety, privacy, and dignity. Hence, anyone building or using AI that affects children must first think through what it will do to them, children must be part of those conversations, and government, companies, teachers, and families must work together to hold each other accountable. The following measures are necessary:

*Enactment of a Comprehensive Child-Centred Legal Framework for AI and Online Safety in Nigeria Mandate Child Rights Impact Assessments for AI System:* Nigeria should enact a comprehensive, child-centred legal framework for online safety and artificial intelligence, drawing on relevant safeguards proposed under the US KIDS Act, the EU AI Act and the COPPA. The framework should extend beyond data protection to address AI-generated harmful content, online exploitation, algorithmic discrimination, addictive platform design and the psychological risks associated with AI chatbots. It should require age-appropriate default safeguards, effective parental controls, transparent and accountable AI systems, and child-rights impact assessments for high-risk applications. The framework should also establish clear duties for technology providers, effective monitoring and enforcement mechanisms, and accessible remedies for children whose rights are violated.

*Improve Digital Literacy among Children and Caregivers:* Governments, private sector and non-profit stakeholders should support AI literacy for children, parents, caregivers, and teachers, so that children learn to use AI in ways that support their development. Parents, caregivers and educators must be supported to learn alongside children, guiding their safe use of AI and exploring its possibilities together.[84]

*Promote Global Cooperation and Standards:* Global cooperation between states should be encouraged so as to hasten the development and implementation of a comprehensive and binding international framework that makes children's rights non-negotiable in AI design, wherever the system is deployed.

[84] UNICEF Office of Strategy And Evidence – Innocenti, Leading Minds Conference: Education In Africa - Outcomes Report, UNICEF Innocenti, Florence, February 2026, <Https://Www.Unicef.Org/Innocenti/Media/12466/File/UNICEF-Innocentilmoutcomes2025-Feb2026.Pdf.Pdf>.