

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Combating Cyberbullying and Child Online Exploitation in Nigeria: Legal Strategies and Enforcement Realities

MAIMUNATU YERIMA IYAWA*  AND JUWAYYRIYA BADAMASIUY** 

ABSTRACT

The rapid expansion of digital technologies and internet access has transformed communication, education, and social interaction globally. This digital revolution, however, has also exposed children to increasing risks of cyberbullying, online grooming, sextortion, child sexual abuse materials (CSAM), and other forms of technology-facilitated exploitation. In Nigeria, the growing number of young internet users, coupled with limited digital literacy and inadequate online safeguards, has heightened children's vulnerability to cyber-related harms. This paper examines the legal and institutional strategies adopted to combat cyberbullying and child online exploitation in Nigeria, with particular emphasis on enforcement realities. Using a doctrinal and comparative legal research methodology, the study analyzes relevant legal frameworks, including the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the Child Rights Act 2003, constitutional provisions, and data protection regulations. It further evaluates the roles of key enforcement institutions such as the Nigeria Police Force, the Economic and Financial Crimes Commission, the Nigerian Communications Commission, and other agencies. The paper identifies significant enforcement challenges, including inadequate technical capacity, weak inter-agency coordination, low reporting rates, societal stigmatization of victims, judicial limitations, and insufficient international cooperation. Drawing lessons from legal and institutional approaches adopted in the United Kingdom, the United States, and South Africa, the study highlights best practices that may strengthen Nigeria's response to online child abuse. The paper concludes by recommending comprehensive legal reforms, with specialized enforcement mechanisms, to ensure effective protection of fundamental rights of children in the digital environment and in cyberspace.

Keywords: Cyberbullying, Child Online Exploitation, Cybercrime, Child Protection, Cyber Law, Enforcement, Nigeria

* Author is a Senior Lecturer at the Faculty of Law, University of Maiduguri, Borno State, Nigeria. ORCID: <https://orcid.org/0009-0003-7311-9395>

** Author is a Professor at the Faculty of Law, Bayero University Kano, Kano State, Nigeria. ORCID: <https://orcid.org/0000-0002-2871-6647>

I. INTRODUCTION

The digital age has revolutionized communication and interaction, bringing both opportunities and risks, particularly for vulnerable groups such as children. Cyberbullying and child online exploitation are increasingly pervasive threats, with victims suffering psychological, emotional, and sometimes physical harm. Cyberbullying involves the use of digital technologies to harass, threaten, or humiliate an individual, while child online exploitation includes grooming, sextortion, trafficking, and the dissemination of child sexual abuse material (CSAM).¹ In recent years, the growth of internet usage and digital communication platforms in Nigeria has been exponential. According to the Nigerian Communications Commission (NCC), internet subscriptions had reached approximately 159 million by August 2023, comprising mobile (GSM), fixed wired and VoIP subscriptions, and continued to increase, reaching approximately 163.8 million by the end of 2023.² A significant portion of these users are young people and school-aged children, who often lack the digital literacy required to navigate the internet safely. Increased access without adequate safeguards has led to a surge in cyber-related threats against minors, particularly in urban and semi-urban areas.³ Online protections for vulnerable populations are therefore critical in Africa, and particularly in Nigeria.⁴ Despite the existence of legal frameworks aimed at combating online abuse, enforcement in Nigeria remains inconsistent and fragmented. Law enforcement agencies often lack the training, tools, and resources to prosecute cybercrimes effectively, especially those involving children. Moreover, societal attitudes, underreporting, and lack of awareness compound the difficulty of addressing these threats comprehensively. The objective of this paper is to examine the effectiveness of Nigeria's legal framework in combating these threats and to evaluate the practical realities faced by enforcement agencies. It also aims to provide actionable recommendations to strengthen legal and institutional mechanisms for child online safety, taking into consideration international best practices and contextual realities.

¹ UNITED NATIONS CHILDREN'S FUND (UNICEF), *Keeping Children Safe Online in the Digital World* (2020).

² NIGERIAN COMMUNICATIONS COMMISSION, *2023 Subscriber/Network Performance Report 4* (2024), <https://ncc.gov.ng/sites/default/files/2025-04/2023-YEAR-END-PERFORMANCE-REPORT.pdf> (reporting 163,838,439 internet subscriptions as at December 2023); see also *Nigeria's Active Mobile Subscribers Hit 220m - NCC*, VANGUARD (Oct. 5, 2023), <https://www.vanguardngr.com/2023/10/nigerias-active-mobile-subscribers-hit-220m-ncc/> (reporting the Commission's figure of 159,034,717 active internet subscriptions as at August 2023).

³ WORLD BANK, *Safe and Inclusive Digital Learning: Policy Guidelines for Protecting Children Online* (2021).

⁴ N. E. Chukwunonso & C. C. Ezeibe, *Policing and Prosecuting Cybercrime in Nigeria: Challenges and Prospects*, 13 AFRICAN JOURNAL OF CRIMINOLOGY AND JUSTICE STUDIES 1 (2020).

II. LEGAL AND REGULATORY FRAMEWORK IN NIGERIA

The theoretical basis for children's digital rights rests on the principle that the rights guaranteed under international human rights instruments, particularly the UN Convention on the Rights of the Child, apply equally in online spaces, thereby requiring states to protect children from digital harms while promoting their safe and meaningful participation in the digital society.⁵

A. Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes Act is Nigeria's principal legislation aimed at tackling offences committed through cyberspace. Sections 23 and 24 are particularly relevant to cyberbullying and child online exploitation. Section 23 criminalizes child pornography and other exploitative acts involving children, including proposing, grooming or soliciting a child through a computer system or network in order to meet the child for sexual activity, and prescribes penalties including fines and imprisonment. Section 24 addresses cyberstalking. As originally enacted, it made it an offence to send, by means of a computer system or network, messages that were grossly offensive, pornographic, indecent, obscene or menacing, or that the sender knew to be false and sent for purposes such as causing annoyance, insult or needless anxiety, and it separately penalised communications intended to bully, threaten or harass another person where they placed that person in fear of death, violence or bodily harm. The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 narrowed the first limb, so that it now reaches messages that are pornographic, or that the sender knows to be false and sends for the purpose of causing a breakdown of law and order or posing a threat to life.⁶

While the Act marked a significant step forward in addressing cybercrime, it has been criticized for its vague language and the absence of specific provisions tailored to children's unique vulnerabilities. For instance, it does not clearly differentiate between cyberbullying of adults and that of minors, which is a critical omission given the psychological and developmental implications of such abuse on children.⁷

B. Child Rights Act 2003

The Child Rights Act (CRA) was enacted to domesticate the UN Convention on the Rights of the Child (CRC). It guarantees children's rights to protection from abuse, neglect, and exploitation. Section 11 of the CRA affirms every child's right to respect for the dignity of his

⁵ A. Ojedokun, *Strengthening Legal Frameworks for Cybersecurity in Nigeria: Lessons from Selected Jurisdictions*, 3 NIGERIAN JOURNAL OF CYBER LAW AND DIGITAL ECONOMY 55 (2021).

⁶ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, §§ 23-24 (Nigeria), *amended by* Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, § 5 (Nigeria).

⁷ F. Adegoke, *Cybersecurity and Enforcement in Nigeria: A Critical Review*, 3 NIGERIAN JOURNAL OF CYBER LAW 45 (2021).

person, under which no child is to be subjected to physical, mental or emotional injury, abuse, neglect or maltreatment, including sexual abuse.⁸ The Act also places obligations on parents, guardians, and government authorities to safeguard children's welfare. However, the application of the CRA is uneven across Nigeria. Under the federal Constitution, children's matters fall within the legislative competence of the States, so the Act does not apply in a State until that State's legislature has enacted it.⁹ Some States are yet to domesticate the CRA, resulting in a patchwork of child protection standards across the country.¹⁰ This legal inconsistency limits the reach and effectiveness of national strategies to combat child online abuse.

C. Constitutional and criminal law provisions

The 1999 Constitution of the Federal Republic of Nigeria provides foundational protections for all citizens, including children. Section 34 guarantees the dignity of the human person and provides that no person shall be subjected to torture or to inhuman or degrading treatment. Section 37 guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. These provisions can be invoked in cases involving violations of privacy and dignity arising from cyberbullying and exploitation. Additionally, the Criminal Code and the Penal Code contain provisions that address traditional crimes such as defamation, indecent assault, and harassment. While these can be extended to cover online acts, the lack of digital-specific provisions often makes prosecution complex and inadequate.

D. Data protection and privacy laws

The Nigeria Data Protection Regulation (NDPR) 2019 was developed to ensure the privacy and protection of personal data. It requires data controllers and processors to implement measures that safeguard personal information. To augment the NDPR, the Nigeria Data Protection Bill was passed by the National Assembly in May 2023 and signed into law by President Bola Ahmed Tinubu on 12 June 2023, creating the Nigeria Data Protection Act (NDPA). The NDPA 2023 provides Nigeria's first comprehensive legal framework for the protection of personal data. Its enactment was widely applauded as aligning Nigeria with international data protection standards, particularly the European Union's General Data Protection Regulation (GDPR) and South Africa's Protection of Personal Information Act (POPIA). One of the most significant

⁸ Child's Rights Act, 2003, § 11(a) (Nigeria).

⁹ Usang Maria Assim, *Why the Child's Rights Act Still Doesn't Apply Throughout Nigeria*, THE CONVERSATION (Sept. 24, 2020), <https://theconversation.com/why-the-childs-rights-act-still-doesnt-apply-throughout-nigeria-145345>.

¹⁰ UNICEF NIGERIA, *Child Rights Act Implementation Status* (2022).

reforms under the NDPA is the establishment of the Nigeria Data Protection Commission (NDPC) as an independent supervisory authority.¹¹

The establishment of the NDPC in 2023 further institutionalized efforts to monitor and enforce data privacy regulations. The regime also extends heightened protection to sensitive personal data, including data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, criminal records or any other sensitive personal information.¹² However, the regime remains limited in its protection of children. Section 31 of the NDPA requires a data controller to obtain the consent of a parent or legal guardian where the data subject is a child, and to apply appropriate mechanisms to verify age and consent,¹³ but there are no further provisions mandating higher standards of protection for minors' data or regulating how technology companies collect and use children's information online. This gap leaves children vulnerable to data breaches, profiling, and exploitation by unscrupulous actors online.

III. INSTITUTIONAL FRAMEWORK FOR ENFORCEMENT

The enforcement of cybersecurity and child protection laws in Nigeria involves a multiplicity of institutions, each with distinct but overlapping mandates.

- **Economic and Financial Crimes Commission (EFCC):** The EFCC is empowered to investigate cybercrime-related financial fraud. It houses a Cybercrime Unit that deals with various internet-related offences. However, its primary focus on financial crimes means that child exploitation cases may not receive adequate attention unless they involve monetary gain.
- **Nigeria Police Force (NPF) Cybercrime Unit:** The NPF has a specialized unit that handles digital crimes, including cyberbullying and exploitation. Despite this, the unit is understaffed and underfunded, lacking the forensic tools and technical know-how needed for thorough investigations. Victims and their families often face bureaucratic hurdles and delayed responses when reporting cases.¹⁴
- **National Information Technology Development Agency (NITDA):** NITDA is tasked with promoting IT development and regulating data compliance. While it has

¹¹ C. C. Ugwu, *Appraisal of the NDPR 2019 and NDPA 2023 in Regulating Data Protection Within Commercial Transactions in Nigeria*, AFRI SOPHIA JOURNAL 8: African Experiment Thought in Experience, vol. 2, no. 4 (Dec. 2025).

¹² *Id.*

¹³ Nigeria Data Protection Act, 2023, § 31 (Nigeria).

¹⁴ M. Ayoade, *Challenges of Prosecuting Cyber Offenses in Nigeria*, 5 AFRICAN LAW REVIEW 89 (2022).

played a role in data privacy through the NDPR, it lacks enforcement power and has minimal engagement in child protection.

- **Nigerian Communications Commission (NCC):** As the telecommunications regulator, the NCC is crucial for obtaining digital footprints and subscriber data that aid in tracking cybercriminals. However, its role is mostly regulatory, and it does not have investigative or prosecutorial powers.
- **Ministry of Women Affairs and Social Development:** This ministry oversees child welfare programmes and collaborates with NGOs to address child abuse. However, its efforts are often under-resourced and limited to awareness campaigns.

Coordination among these agencies is weak. There are jurisdictional conflicts, and the lack of a centralized child cyber safety unit hinders efficient response to threats. Moreover, most agencies lack specialized units or personnel trained specifically in handling child online exploitation cases.

IV. ENFORCEMENT REALITIES AND CHALLENGES

Despite the existence of legal and institutional frameworks, the enforcement of laws against cyberbullying and child online exploitation in Nigeria faces multifaceted challenges. These challenges cut across institutional limitations, legal loopholes, societal attitudes, and technical constraints.

A. Inadequate law enforcement capacity

One of the major impediments to effective enforcement is the lack of trained personnel within the police and other enforcement agencies.¹⁵ The specialized skills required to investigate cybercrimes, such as digital forensics, encryption analysis, and cyber surveillance, are scarce within the Nigerian law enforcement community. According to the United Nations Office on Drugs and Crime,¹⁶ only a small fraction of officers in Nigeria's cybercrime units possess formal training in digital evidence handling. Furthermore, forensic laboratories are under-equipped, and there is limited access to sophisticated technologies for identifying perpetrators who use anonymization techniques such as Virtual Private Networks (VPNs) or the dark web. As a result, most reported cases of child online abuse remain uninvestigated or unprosecuted, allowing perpetrators to act with impunity.

¹⁵ INTERNATIONAL TELECOMMUNICATION UNION, *Child Online Protection Guidelines for Policymakers* (2021).

¹⁶ UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Online Child Exploitation and Abuse: Comparative Global Approaches* (2021).

B. Poor interagency coordination

Nigeria's cybersecurity and child protection landscape is characterized by institutional fragmentation. Agencies such as the EFCC, NPF, NITDA, and NCC often operate in silos, with minimal information sharing or coordinated action. The absence of a central coordinating body has led to duplicative efforts and confusion over jurisdiction, particularly when cases involve cross-border or inter-state digital activities. In many instances, the lack of clarity on which agency should take the lead on a case results in delay or outright neglect of investigations. This disjointed structure diminishes the effectiveness of Nigeria's response to online child exploitation.

C. Low reporting rates and victim stigmatization

Cultural and societal factors also play a significant role in limiting the enforcement of legal protections. Many victims of cyberbullying and online exploitation, and their families, are reluctant to report incidents due to fear of stigmatization or reprisal. In cases involving child sexual abuse material or sextortion, the social stigma attached to perceived immorality further discourages reporting, especially among girls in conservative communities.¹⁷ Moreover, the lack of awareness about digital rights and reporting mechanisms means that many families do not know where or how to seek redress. This has created a significant gap between the existence of legal protections and their actual utilization.

D. Weak judicial responses

Generally, when cases reach the courts, prosecution is often slow and outcomes unsatisfactory. Delays in court proceedings can span months or years, leading to a loss of evidence, waning public confidence in the system and, at times, the acquittal of offenders on technicalities. The practice of ordering trials *de novo* and of permitting interlocutory appeals often results in unnecessary delay, prolonging the determination of substantive cases and undermining the expeditious administration of justice.¹⁸ In addition, the judiciary lacks adequate expertise in handling cyber-related offences, there is no specialized cybercrime court or designated child protection bench in most jurisdictions, and inconsistent interpretation of the laws, particularly the Cybercrimes Act, leads to divergent judgments. These shortcomings highlight the need for judicial training and for specialized courts or tribunals to deal with cyber offences involving children.

¹⁷ A. I. Ajayi & T. M. Fashola, *Stigma and the Silent Cry: Reporting Barriers Among Survivors of Child Sexual Abuse in Nigeria*, 26 AFRICAN JOURNAL OF REPRODUCTIVE HEALTH 84 (2022).

¹⁸ See *Dada v. Bankole* (2008) 1 SC (Pt. III) 219 (Nigeria).

E. Limited international cooperation

Due to the global nature of cybercrime, effective enforcement requires transnational cooperation. Unfortunately, Nigeria's ability to collaborate with international law enforcement bodies such as INTERPOL or Europol is hampered by limited diplomatic agreements and bureaucratic bottlenecks. This is especially problematic in cases where perpetrators or hosting platforms are in jurisdictions outside Nigeria. Although Nigeria acceded to the Budapest Convention on Cybercrime in July 2022, practical cooperation under this framework remains minimal due to lack of technical capacity and legal harmonization.¹⁹ This deficiency hampers the successful prosecution of cybercriminals who exploit children across borders using platforms hosted in other countries.

V. COMPARATIVE LEGAL APPROACHES

Examining legal strategies from other jurisdictions offers valuable insights for strengthening Nigeria's response to cyberbullying and child online exploitation.²⁰ Countries such as the United Kingdom, the United States, and South Africa have adopted comprehensive and often innovative approaches that can inform Nigeria's policy and legislative reforms, which underlines the need to adopt international best practices in policy design for child online safety. Livingstone and Bulger provide a theoretical foundation for understanding children's digital rights, emphasizing that the principles of the United Nations Convention on the Rights of the Child (UNCRC) must be extended to the digital environment to ensure children's protection, participation, and development in an increasingly connected world.²¹

A. United Kingdom

The UK has developed a robust legal and policy framework to address online harm. The Online Safety Act 2023, which received Royal Assent on 26 October 2023, requires technology companies to take proactive measures against harmful content, including child sexual exploitation and abuse (CSEA) material and cyberbullying. The Act imposes safety duties on regulated online services in relation to illegal content, which have applied since 17 March 2025, and empowers Ofcom, where the statutory conditions are met, to require providers to deploy accredited or appropriately developed technology to identify, prevent access to, and remove

¹⁹ Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185; COUNCIL OF EUROPE, *Budapest Convention on Cybercrime: Status of Signatures and Ratifications* (2023), <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>.

²⁰ UNICEF, *supra* note 1.

²¹ Sonia Livingstone & Monica Bulger, *A Global Research Agenda for Children's Rights in the Digital Age*, 8 JOURNAL OF CHILDREN AND MEDIA 317 (2014), <https://doi.org/10.1080/17482798.2014.961496>.

CSEA content.²² Ofcom, the communications regulator, enforces these duties and may fine companies up to £18 million or 10 per cent of their qualifying worldwide revenue, whichever is greater, for non-compliance.²³ The UK also has a specialized command within the National Crime Agency (NCA), the Child Exploitation and Online Protection (CEOP) Command, which is dedicated to protecting children from sexual exploitation and abuse, including online. Additionally, courts in the UK have issued significant judgments under laws such as the Malicious Communications Act 1988 and the Protection from Harassment Act 1997, both of which have been used to prosecute cyberbullying and online harassment.

B. United States

In the United States, a combination of federal and state laws governs cyberbullying and online child protection. The Children's Online Privacy Protection Act (COPPA) requires websites and online services to obtain verifiable parental consent before collecting personal data from children under 13. The PROTECT Our Children Act provides federal funding to task forces combating technology-facilitated child exploitation. The U.S. also has strong institutional support for enforcement: agencies such as the FBI and Homeland Security Investigations (HSI) have dedicated cybercrime units. In several states, cyberbullying laws explicitly address school-related digital harassment, and some states impose criminal penalties for repeated or severe offences.²⁴ In *Packingham v. North Carolina*,²⁵ the Supreme Court considered a North Carolina law restricting registered sex offenders' access to social-media websites, described social-media platforms as among the most important places for the exchange of views, and struck the law down as incompatible with the First Amendment. It is submitted that there should be explicit restrictions on the kinds of goods and services that may be advertised on social media.

C. South Africa

South Africa's Cybercrimes Act 2020 criminalizes cyber harassment, the electronic distribution of intimate images without consent, and child pornography. The Act provides clear definitions and penalties, offering more legal clarity than many older cybercrime laws. South Africa's Specialised Commercial Crimes Courts also hear cybercrime prosecutions, and the country trains its judiciary and prosecutors in digital crime handling. The South African Police Service (SAPS) Cybercrime Unit also collaborates with global partners and maintains a dedicated

²² Online Safety Act 2023, c. 50, §§ 10, 121 (UK); see CMS, *Online Safety Act: Illegal Content Duties Are Now in Force* (Mar. 2025), <https://cms.law/en/gbr/legal-updates/online-safety-act-illegal-content-duties-are-now-in-force>.

²³ Online Safety Act 2023, c. 50, sch. 13, para. 4 (UK).

²⁴ SAMEER HINDUJA & JUSTIN W. PATCHIN, *BULLYING BEYOND THE SCHOOLYARD: PREVENTING AND RESPONDING TO CYBERBULLYING* (2d ed. 2020).

²⁵ *Packingham v. North Carolina*, 582 U.S. 98, 104, 108 (2017).

platform for reporting online exploitation. Moreover, the country has invested in digital literacy campaigns to educate parents, teachers, and children about safe online behaviour.

D. Key lessons for Nigeria

i. Establishment of a centralized, specialized cybercrime and child protection agency or unit

One major lesson from jurisdictions such as the United Kingdom and the United States is the importance of creating specialized institutions dedicated to addressing cybercrime and child online exploitation. Agencies such as the CEOP Command in the UK have demonstrated the effectiveness of a centralized approach in coordinating investigations, intelligence gathering, victim support, and interagency collaboration. Nigeria can benefit from establishing a dedicated national child online protection unit with clearly defined mandates and adequate technical resources to ensure prompt and effective responses to online threats against children.

ii. Enactment of clearer, child-specific cybercrime laws

Nigeria's current cybercrime framework provides general protection against online offences but lacks comprehensive child-specific provisions. Lessons from countries such as South Africa and the United States show the value of legislation that clearly defines offences such as cyberbullying, online grooming, sextortion, and the distribution of child sexual abuse materials. Enacting clearer and more targeted laws would eliminate ambiguities, facilitate prosecution, and provide stronger legal protection for children in digital environments.

iii. Imposition of statutory obligations on technology platforms to prevent and respond to abuse

Modern approaches to child online protection increasingly place responsibility on technology companies to protect users from harmful content and online exploitation. The United Kingdom's Online Safety Act 2023, for example, requires online platforms to identify, remove, and report harmful content proactively. Nigeria can adopt similar measures by imposing legal obligations on social media companies, internet service providers, and digital platforms to implement safety measures, age-verification systems, content moderation mechanisms, and efficient reporting procedures.

iv. Investment in judicial and law enforcement training for handling digital evidence

Effective enforcement of cybercrime laws depends largely on the capacity of investigators, prosecutors, and judges to understand and manage digital evidence. Countries with successful cybercrime enforcement systems invest heavily in specialized training on digital forensics,

cyber investigations, electronic evidence management, and emerging technologies. Nigeria should strengthen the capacity of law enforcement agencies and judicial officers through continuous professional training and the provision of modern forensic tools and technological infrastructure.

v. Expansion of public awareness and digital literacy campaigns

Prevention remains one of the most effective strategies for combating cyberbullying and child online exploitation. Public awareness programmes in countries such as South Africa and the United Kingdom have helped educate children, parents, teachers, and communities on online safety and responsible internet use. Internet access and digital literacy should be regarded not merely as economic tools, but as vital legal and civil rights. Nigeria should intensify digital literacy campaigns through schools, media organizations, religious institutions, and community groups to promote awareness of online risks, reporting mechanisms, privacy protection, and safe digital behaviour among children and young people.

These practices demonstrate that effective enforcement depends not only on legal provisions but also on institutional preparedness, stakeholder collaboration, technological capacity, and public awareness.

VI. STRATEGIC RECOMMENDATIONS

To combat cyberbullying and child online exploitation effectively, Nigeria must implement a multifaceted strategy that integrates legal, institutional, technological, and societal interventions. The following recommendations are proposed.

A. Legal reform and legislative clarity

There is an urgent need to amend the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 to include specific provisions addressing cyberbullying of minors and various forms of child online exploitation. These amendments should incorporate clear definitions and penalties aligned with international standards such as the Lanzarote Convention and the Budapest Convention. Moreover, federal advocacy must be intensified to ensure full domestication and implementation of the Child Rights Act in all States of the federation. Harmonizing state-level laws with national cybersecurity and child protection frameworks will eliminate the current legal fragmentation and create a unified standard of protection.

B. Strengthening enforcement institutions

Enforcement agencies, particularly the Nigeria Police Force, the EFCC, and the judiciary, require dedicated cybercrime units with specialized training in digital evidence gathering,

forensics, and victim-sensitive investigations. Equipping these units with up-to-date technology and forensic laboratories is essential for effective investigation and prosecution. Additionally, the creation of a National Child Cyber Safety Coordination Center (NCCSCC) under the Federal Ministry of Justice or the Federal Ministry of Communications, Innovation and Digital Economy would enhance multi-agency collaboration and serve as a hub for information sharing, case tracking, and victim support.

C. Public awareness and digital literacy

Government agencies, in collaboration with NGOs and the media, should launch national awareness campaigns on the dangers of cyberbullying and online exploitation. These campaigns should target children, parents, teachers, and community leaders, using culturally appropriate messaging. Incorporating digital citizenship and online safety into school curricula at all levels will equip children with the knowledge and skills to navigate the digital environment safely. Special attention should be given to educating children on privacy, consent, and how to report online abuse.

D. Private sector accountability

Technology companies, including telecommunications operators and social media platforms, must be held accountable for user safety. Legislative reforms should require platforms to:

- deploy AI tools for detecting and removing CSAM;
- provide age-appropriate content filters; and
- ensure swift reporting mechanisms for abusive content.

Collaboration with these platforms can also enhance law enforcement's ability to trace and investigate perpetrators while respecting data protection standards.

E. International cooperation

Nigeria should leverage its membership of global cybersecurity and human rights frameworks to facilitate information exchange, capacity building, and joint investigations. Strengthening its legal and diplomatic infrastructure to utilize mutual legal assistance treaties (MLATs) will also improve cross-border enforcement capabilities. Furthermore, partnerships with international organizations such as INTERPOL, Europol, and UNICEF can support Nigeria with technical resources, training, and access to global threat intelligence databases.

VII. CONCLUSION

Cyberbullying and child online exploitation represent urgent threats to the safety, dignity, and development of children in Nigeria's increasingly digital society. Despite existing legal instruments such as the Cybercrimes Act 2015 and the Child Rights Act, enforcement realities reveal significant shortcomings, ranging from institutional capacity gaps to limited awareness and weak judicial responsiveness. A comparative analysis of legal strategies in countries such as the United Kingdom, the United States, and South Africa underscores the importance of an integrated approach combining robust legislation, institutional specialization, public education, and global cooperation. These lessons are vital for Nigeria as it grapples with the growing complexity of technology-facilitated crimes against children. To bridge the enforcement gap, Nigeria must commit to comprehensive legal reform that explicitly addresses child-specific cyber risks, establish specialized cybercrime and child protection agencies, invest in public awareness and digital literacy, and ensure accountability within the private technology sector. It must also strengthen cross-border enforcement mechanisms through international cooperation. Because cyberbullying and the online exploitation of children are serious violations of children's fundamental rights, with national, regional and international implications, they require a more complex understanding and multi-agency responses. Ultimately, safeguarding children in the digital age is not just a legal or technological obligation; it is a moral and developmental imperative. An effective legal framework, matched with proactive enforcement and societal engagement, will ensure that Nigeria meets its national and international commitments to protect its most vulnerable population from online harm.
