Fountain University Law Journal Vol. 2 No. 4, 2025

THE LEGAL REGIME OF CYBERBULLY AND VICTIM PROTECTION IN NIGERIA

By

Lateef A. Adeleke PhD*

&

Zainab A. Oluwo**

Abstract

The rise of digital technology and social media has transformed communication, but it has also given rise to new forms of harm, particularly cyberbullying. This paper critically examines the legal and institutional framework for addressing cyberbullying in Nigeria, with a focus on how victims are protected under existing laws. The paper adopts a doctrinal legal research methodology, being primarily qualitative and library-based, relying on both primary and secondary sources. Drawing from statutory provisions, case law, and international instruments, the study explores how Nigerian laws such as the Cybercrimes Act 2015, Child's Rights Act 2003, NDPR 2019, and the Constitution respond to online abuse and digital harm faced by victims. The paper also evaluates the role of key institutions like the Nigeria Police Force, NITDA, NCC, NSCDC, and the Computer Professionals Registration Council, while comparing Nigeria's approach with global standards such as the Budapest Convention and the UNCRC. Through real-life examples, unreported court cases, and victim testimonies, the paper highlights the practical challenges of enforcement, such as poor awareness, function overlap among institutions, and lack of data protection literacy among citizens. Finally, the study finds that while Nigeria has taken important legal steps, enforcement mechanisms remain weak, and victim support systems are underdeveloped. It recommends cordial institutional coordination, updated digital literacy policies, and targeted reforms to make cyberbullying laws more responsive and inclusive.

Keywords: **Cyberbullying, Cybercrimes, Cyber stalking, Social Media Harassment, Victim Protection.**

1.0 INTRODUCTION

The digital revolution has permeated every aspect of human life; the rapid growth of digital technology and the spread of the internet have significantly changed how people communicate around the world.[1] With the advanced use of smartphones and social media platforms such as

*Associate Professor, College of Law, Fountain University, Osogbo Nigeria.

** A Law graduate from Fountain University, Osogbo, Nigeria.

[1]M. Aliyu, 'Cyberbullying in Tertiary Education institutions in Nigeria: Modes, Levels, Consequences and Causal Factors', *SOS Poly: Journal of Science and Agriculture* (2022) (4) 2536-7161.

Facebook, Twitter (X), WhatsApp, and Instagram, many Nigerians, especially the Generation Z,[2] have become more engaged in online spaces than ever. Social media in all of its forms has changed the world a lot. It has connected people personally and professionally, given friends and loved ones another avenue of contact, and brought people from all corners of the planet together.[3] While this platform offers a space for social interactions, it shapes education, business, and political engagement. Despite the foregoing prowess, the internet is now negatively used by those who spitefully hurt others from behind the shield of anonymity[4] and verbally attack anyone at any time from any place. As the digital landscape continues to evolve, so too does the complexity of cyberbullying.[5] New forms of online harassment, such as doxxing (publishing private information online), sextortion (using explicit images or videos to extort victims), and online hate speech, present a tapestry of challenges in combating this persuasive issue.[6] It is worthy of note, that traditional bullying and Cyberbullying cannot be confused as the same. Several studies suggest it could cause harm far above and beyond traditional bullying.[7] On the contrary as opposed to traditional bullying, cyberbullying occurs in a digital space, where it can be anonymous, difficult to trace, and accessible to both domestic and foreign audiences. This intensifies the victims psychological trauma, who in most cases suffer anxiety, depression and, in extreme cases, suicide.[8] Unfortunately, a number of these occurrences remain unreported due to some factors, including a lack of public awareness about the issue, difficulty in identifying offenders and our legal system is still developing. While the Cybercrime (Prohibition, Prevention) Act 2015 addresses online harassment, much is still left to be desired as there gaps in enforcement and public awareness, regarding the laws surrounding this harassment. The Act does not explicitly cover emerging forms of cyberbullying such as trolling, outing, and doxxing, leaving many victims without clear legal protection.

While there is the need for improvement, the Cybercrime Act, 2015[9] remains a harbinger of hope for victims of cyberbully, as it provides a framework for the prevention and prosecution of cybercrimes in Nigeria today. There have been cases in Nigerian courts where these provisions

[2] Generation Z (Gen Z) refers to the demographic cohort born roughly between 1997 and 2012. They are characterized as digital natives who have grown up with access to the internet, smartphones, and social media, shaping their communication styles, learning habits, and social values.
[3] D. Morris, 'The Rise of Social Media: How the World Became Connected' (18 February 2022) https://www.shropshirestar.com/entertainment/2022/02/18/the-rise-of-social-media-how-the-world-became-connected/ accessed 30 April 2025.
[4] N.E Wilard, *Cyberbullying and cyber threats.* (2nd edn, Research Press, Illinois 2007) 42.
[5] O.O. Olasanmi, Y.T. Agbaje and M.O. Adeyemi, 'Prevalence and Prevention Strategies of Cyberbullying Among Nigerian Students', *Open Journal of Applied Sciences* (2020) (10) (6) 351-363. https://doi.org/10.4236/ojapps.2020.106026 accessed 30 April 2025.
[6] S.D. Hazlewood and S. Koon-Magnin, 'Cyber Stalking and Cyber Harassment Legislation in the United States. A qualitative Analysis', *International Journal of Cyber Criminology* (2013) (7) 155-168.
[7] D. Cross, L. Lester and A. Barnes, 'A Longitudinal Study of the Social and Emotional Predictors and Consequences of Cyber and Traditional Bullying Victimization', *International Journal of Public Health* (2015) (60) (2) 207-217.
[8] J.C. Lafferty, 'Anonymity, the internet, and the Legal Challenges of Cyberstalking', *Berkeley Technology Law Journal* (2014) (29) (1) 175-222.
[9] Cybercrimes *(Prohibition, Prevention, etc.)* Act 2015, s24 (2).

have been applied. In *AG of the Federation* v. *Ayan Olubunmi*,[10] the Federal High Court in Ado-Ekiti, Ekiti State, sentenced Ayan Olubunmi to two years imprisonment and a fine of N500,000 for posting the nude photos of his ex-lover, Aare Monica, on Facebook. Ayan had threatened to share explicit images on social media when Monica ended the relationship between them in 2017. Despite Monica's plea and an offer of N200,000 as an inducement, Ayan posted the pictures as he threatened. The court found Ayan guilty of violating the Cybercrime Act of 2015, and the judge described the act as disgraceful and barbaric. While the maximum penalty for the offense was a N7 million fine and a three-year prison term, Ayan was sentenced to a two-year prison term and a fine of N500, 000. However, despite such success, many victims continue to face challenges in accessing justice, and the legal process remains slow. Enforcement of the law is still inconsistent, with victims often unaware of their rights.[11]

2.0 WHAT IS CYBERBULLY?

There is no commonly agreed definition of cyberbullying, however much juristic ink has flown in a bid to provide a universal definition of this keyword. Cyberbullying simply put, is bullying which occurs online. It is the persistent and deliberate harassment that causes harm to a targeted individual.[12] Cyberbullying and traditional bullying although similar in terms of forms and techniques they have their differences.[13] Victims of cyberbullying may not know who is targeting them, or why.[14] The aggressor can cloak his or her identity using anonymous accounts and unauthentic screen names. Secondly, the hurtful actions of those who cyberbully can more easily go viral, that is, a large number of people in the world can participate in the victimization or at least find out about the incident with a few impressions.[15]

Cyberbullying is bullying which uses e-technology as a means of victimizing others. It is the use of internet media or mobile technologies such as email, chat room discussion programs, mobile phone cameras, web pages, text messages, with the intention of harming other persons. The methods used includes texting offensive messages on mobile phones, with offender showing the message to others before sending it to the victim, sending threatening emails and forwarding a confidential email to address book contacts, thus publicly humiliating the first sender.[16]

3.0 TYPES OF CYBER BULLYING

[10] *Attorney General of the Federation v Ayan Olubunmi* (2018) FHC/AD/17C/2017 (Fed High Ct) unreported.
[11] Trusted Advisors, 'Understanding Cyberbullying Laws in Nigeria: Victim Protection and Accountability' (12 April 2025) https://trustedadvisorslaw.com/understanding-cyberbullying-laws-in-nigeria-victim-protection-and-accountability/ accessed 30 April 2025.
[12] R. Bashir, 'Legal consequences of social media: *Defamation, privacy, and cyberbullying*' Trusted Advisors Law (2023) < https://trustedadvisorslaw.com/legal-consequences-of-social-media-defamation-privacy-and-cyberbullying/ accessed 30 April 2025.
[13] L.R, Betts, '*Cyberbullying Approaches, Consequences and interventions* (Palgrave Macmillan 2016) 29.
[14] D.J Meter and S.Bauman,'Moral disengagement about cyberbullying and parental monitoring: Effects on traditional bullying and victimization via cyberbullying involvement' *The Journal of Early Adolescence* (2018) (38) (3) 303-326.
[15] J.W. Patchin and S. Hinduja, 'Bullies move beyond the schoolyard: a preliminary look at cyberbullying'. *Youth Violence and Juvenile Justice* (2006) 4 (2) 148-169.
[16] M. Snider and K. Borel, 'Stalked by a Cyberbully' *Maclean's*, (2004) (117) 76-77

3.1 Harassment

Harassment[17] is a sustained constant and intentional form of bullying it involves sending offensive, rude, or insulting messages to an individual through emails, texts or social media platforms. Such persistent behavior can cause significant emotional distress to the victim. A case study of this form of cyberbullying is the Monica Lewinsky[18] Monica Lewinsky, a former White House intern, became the subject of extensive public shaming and cyber harassment following the revelation of her affair with then-President Bill Clinton in the late 1990s. As details of the affair were leaked to the media, Lewinsky's life was thrust into the public spotlight, leading to widespread online abuse. In the early days of the internet, this scandal was amplified through email chains, early websites, and public forums where she was relentlessly mocked, ridiculed, and humiliated. The harassment was not only confined to online spaces but also extended to the media and broader public discussions, creating an atmosphere of global public shaming.

3.2 Impersonation

Impersonation,[19] also known as identity theft, is a significant form of cyberbullying where the perpetrator pretends to be someone else online, often with malicious intent. This can involve creating fake social media profiles, hacking into personal accounts, or otherwise assuming the victim's identity to deceive, harass, or harm them. The goal of impersonation is typically to undermine the victim's reputation or to cause emotional distress. The bully might send offensive messages, post inappropriate content, or make defamatory remarks masquerading as the victim. Since the impersonator is using the victim's identity, the actions are often taken seriously by others, causing confusion, embarrassment, and sometimes even legal consequences, for example perpetrators create fake profiles impersonating Nigerian minors, often using their photos or personal information. They can post misleading or harmful content, damaging the victims reputation and relationships.[20]

3.3 Cyber Stalking

Cybercrime (Prohibition, Prevention, etc.) Act 2015 is the mainline legislation in Nigeria tackling cybercrimes including cyber stalking, particularly section 24 of the Act, The provisions of the Act apply throughout the Federal Republic of Nigeria.[21] Under the Act, cyber stalking is defined as a course of conduct directed at a specific person that would cause a reasonable person to feel fear. Cyber stalking is a severe form of cyberbullying where an individual uses the internet or other digital platforms to repeatedly harass or monitor someone. It goes beyond mere online harassment,

[17] Kowalski RM, Giumetti GW, Schroeder AN and Lattanner MR 2014. 'Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin 140 (4):1073-1137.
[18] Wikipedia , 'Clinton- Lewinsky scandal' *Wikipedia* (2025) .<https://en.wikipedia.org/wiki/clinton%E2%80%93Lewinsky_scandal > accessed 30 April 2025
[19] Calmerry, '10 types of cyberbullying and how to protect yourself' *Calmerry Blog* <https://calmerry.com/blog/self-care/types-of-cyberbullying> accessed 30 April 2025.
[20] S. Hinduja and J.W. Patchin, 'Cyberbullying and Cyberbullying Policy Legislation' in D.G. Singer and J.L. Singer (eds), *Handbook of Children and the Media* (2nd edn, Sage Publications, 2012) 603-620.
[21] Federal Republic of Nigeria, Cybercrimes (*Prohibition, Prevention, etc.*) Act 2015, s.2, s.58

cyber stalking typically involves a pattern of behavior designed to control, intimate the victim.[22] In cyber stalking, the perpetrator may engage in behaviors such as sending threatening emails or messages, monitoring the victim's online activities, tracking their locations or even creating fake online accounts to spread malicious rumors or threats and monitors their online activities without their consent this invasion of privacy can be deeply unsettling and frightening.[23]

4.0 THEORETICAL FRAMEWORK

4.1 Social Learning Theory

Social learning Theory suggests that aggressive and deviant behaviors, including cyberbullying are learned through interaction with external environment, particularly through exposure to socially deviant role models and the reinforcement of maladaptive behaviors. Bandura argued that when individuals observe aggressive behaviors being rewarded or reinforced such a child bullying others and receiving positive reinforcement from peers (e.g laughter, joining in or approval) they are more likely to repeat these behaviors.[24] The reinforcement, in this case, strengthens the behavior and makes it more likely to occur again. When applied to cyberbullying, it raises the question of whether the reinforcement of such behaviors occurs in the same way as it does in physical settings. In the online environment, behaviors like cyberbullying might be reinforced through social approval on platforms like social media, where actions such as "liking" a post or sharing a hurtful comment might encourage the perpetrator to continue the behavior. The external validation or reinforcement from peers in the virtual space could, therefore serve as a powerful motivator for individuals to engage in further aggressive or harmful actions.[25]

Social learning theory is relevant in this work because it suggests that individuals especially young people might engage in cyberbullying because they have observed it in their social environments either offline or online and receive reinforcement from peers. This could explain why cyberbullying is so prevalent on social media platforms where harmful behaviors are sometimes endorsed.

5.0 LEGAL FRAMEWORK OF CYBERBULLYING IN NIGERIA

In Nigeria today, the activities of cyber criminals have become a threat to the society.[26] With the advent of information age, legislatures have been struggling to redefine laws that fit crimes committed by cyber criminals.[27] Initially, there were no specific and adequate laws in Nigeria to

[22] H.M. Shambhavee, 'Cyber-Stalking: Threat to People or Bane to Technology' *International Journal of Trend in Scientific Research and Development* [2019] (3)(2) 353
[23] M.L. Ybarra, M. Diener-West and P.J. Leaf, 'Examining the Overlap in Internet Harassment and School Bullying: Implications for School Intervention' *Journal of Adolescent Health* [2007] (41) 42–50
[24] A. Bandura, *Social Foundations of Thought and Action*: *A Social Cognitive Theory* (Prentice-Hall, Englewood Cliffs, NJ, 1986)
[25] D.L. Espelage, M.A. Rao and R.G. Craven, 'Theories of Cyberbullying' *Journal of School Violence* [2013] (12)(3) 183–202
[26] R. Oke, 'Cyber Capacity Without Security: A Case Study of Nigeria's National Policy for Information Technology (NPFIT)' *The Journal* of *Philosophy, Science and Law* [2012] 12–14
[27] L. Ani, 'Cybercrime and National Security: The Role of the Penal and Procedural Law' in E. Azinge (ed), *Law and Security in Nigeria* (Nigerian Institute of Advanced Legal Studies Press, 2011) 197–234

combat computer crimes.[28] This led to the creation of an enabling environment for criminals to freely operate without any law to combat their criminal activities.[29] It is a general principle of law that an uncodified crime is not punishable, as provided in Section 36 (12) of the 1999 Constitution of the Federal Republic of Nigeria.[30] The factors involved in the prosecution of a crime under the Nigerian law emanates from one major source, legislation. As a result of this, the Cybercrime Act 2015 has been enacted for the prohibition, prevention, detection, and prosecution of cybercrimes and for other related matters. Aside the new Cybercrime Act, there are laws that indirectly relate to the prosecution of cybercriminals.

The primary cybercrime legislation in Nigeria is the cybercrime Act 2015[31] which was signed into law on May 15, 2015 with 8 Parts, 59 Sections and 2 Schedules and most of its provisions are similar with that of the Budapest convention on Cybercrimes which further gives effect to the 2011 ECOWAS directive on fighting cybercrimes.[32] It is imperative to state that due to the sensitive nature of cyber offences and the trans-boundary nature of the cyberspace, the Cybercrime Act maintains natural application that works to the exclusion of the state houses of assembly.[33] The Act consist of the following parts: Part I. Object and Application, Part II. Protection of Critical National Information infrastructure Part III. Offences and Penalties, Part IV Duties of Financial Institutions, Part V. Administration and Enforcement, Part VI. Arrest, Search, Seizure and Prosecution, Part VII. Jurisdiction and International Cooperation, Part VIII. Miscellaneous.

5.1 Constitution of the Federal Republic of Nigeria

The first point of call for cybercrime protection under the Nigeria legal jurisprudence is the 1999 Constitution of the Federal Republic of Nigeria (as amended), Section 37 of the Constitution provides that the privacy of citizens, their homes, correspondence telephones conversations and telegraphic communication is hereby guaranteed and protected.[34] According to the Constitution, the individual's right to privacy is sacrosanct and it can only be fettered by laws made by democratically enabled public authorities in the interest of national security, public safety or economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or for the protection of the rights and freedom of others.[35] In the interest of defense, public safety, public order, public morality or public health; or for the purpose of protecting rights and freedom of other persons assume from the above, the right to privacy of an individual even when protected by the constitution can be compromised by any act of the federation which seeks to protect public safety, order and interest thus, enforcement of the right of privacy, under the

[28] R. Ehimen and A. Bola, 'Cybercrime in Nigeria' *Business Intelligence Journal* [2010] 93–98
[29] Ibid
[30] Federal Republic of Nigeria, *Constitution of the Federal Republic of Nigeria* (*as amended*) [1999], s.36(12)
[31] Hereinafter referred to as "the Act"
[32]U. Joseph, 'Legislative Framework for Cybercrime in Nigeria: Current Status, Issues and Recommendation' *Open Access Law* [n.d.] https://oa/.law accessed 30 April 2025
[33] F. Eboibi, 'A Critical Exposition of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act 2015' *DELSU Law Review* [2019] (5)
[34] Federal Republic of Nigeria, *Constitution of the Federal Republic of Nigeria* (as amended) [1999], s.37
[35]N.O. Umejiaku and M.I. Anyaegbu, 'Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria' *International Journal of Computer and Technology* [2016] (15)(10) 7130–7139.

constitution may not be readily obtainable an individual may need to seek redress under other applicable laws[36].

5.2 Criminal Code Act (Southern Nigeria) and Penal Code Act (Northern Nigeria)

The Criminal Code Act[37] and Penal Code Act[38] are the major criminal laws in Nigeria and are applicable to different region (The western region and Northern region respectively). They criminalize the distribution and projection of obscene articles. These laws and provisions apply to cyberbullying cases that involve the dissemination of obscene content. Chapter 21A and 17 of the Criminal Code Act provide a legal framework for addressing obscene publications and offence related to posts and telecommunications, respectively. Chapter 21A of the Criminal Code Act defines 'obscene articles as any material that is capable of being viewed, read, or heard, and tends to deprave and corrupt individuals who may come into contact with it (Chapters 21A, 233 B).

This definition lays the precedent for identifying and classifying content that promotes cyberbullying and falls within the scope of law. According to Section 233C of Chapter 21A, an article is considered obscene if, taken as a whole, its effect tends to corrupt or deprave individuals (Chapters 21A and 233C). This provision establishes a standard by which the offensiveness and harm caused by cyberbullying content can be assessed. To address the distribution of obscene articles, Section 233D of Chapter 21A stipulates that individuals who distribute or project such material, whether gain or not, commit an offense (Chapters 21A and 233D). This offense carries penalties, including fines not exceeding N400, imprisonment for a term not exceeding three years, or both. These provisions can be used to hold cyberbullies accountable for their actions to discourage the dissemination of harmful content.

Like the Criminal Code Act, the Penal Code Act addresses the question of obscene materials in Nigeria. Section 463 of Chapter 34 which relates to posts and telecommunications focuses on the act of sending dangerous or obscene items. According to the Section, individuals who intentionally send items by that have the potential to cause harm or enclose obscene materials commit offenses. The items mentioned include those that are likely to cause injury to a person or object during conveyance, as well as those that contain obscene books, pamphlets, papers, gramophone records, drawings, paintings, representations, or figures. The punishment for this offense is imprisonment for up to one year, a fine, or both, as determined by the court. While these Acts (Criminal Code and Penal Code) address the dissemination of obscene materials through post and telecommunications, they do not mention cyberbullying which occurs primarily through digital means such as social media platforms, messaging applications, and online forums. However, by

[36] I.J. Viko, 'Of the Legal and Institutional Framework for Fighting Cybercrime in Nigeria' *International Journal of Comparative Law and Legal Philosophy* [2021] https://www.nigerianjournalsonline.com/index.php/IJOCLLEP/article/view/1686 accessed 30 April 2025

[37] Federal Republic of Nigeria, *Criminal Code Act*, Cap.77 Laws of the Federation of Nigeria (LFN) [1990], ss.21A, 232B, 233C, 233D

[38] Federal Republic of Nigeria, *Penal Code Act*, Cap.34 Laws of the Federation of Nigeria (LFN) [1990], s.463

employing these provisions, Nigerian authorities can take legal action against individuals who engage in cyberbullying by sending harmful or obscene content through a postal system.[39]

5.3 The Child Rights Act 2003

The child Rights Act 2023 is a foundational statute in Nigeria's legal framework for the protection of Children. Enacted to domesticate the United Nations Convention on the Rights of the Child (UNCRC) and the African charter on the Rights and welfare of the Child, the Act Provides a Comprehensive legal Structure that guarantees the rights and welfare of children in Nigeria. It is particularly significant in addressing issues of online abuse, exploitation and cyberbullying which disproportionately affect minors.

Section 11 of the Act is particularly relevant, as it protects children against all forms of abuse, violence, and exploitation, stating that "Every child is entitled to respect for the dignity of his person, and accordingly, no child shall be (a) subjected to physical, mental or emotional injury, abuse, neglect or maltreatment, including sexual abuse.[40] This provision is broad enough to include forms of cyberbullying, digital harassment, and online exploitation of children, even though the Act does not explicitly mention "cybercrime" or "cyberbullying." Moreover, Section 14(1) reinforces the child's right to survival and development, which is threatened by persistent cyber abuse.

Section 32 also protects a child from sexual exploitation and use in pornography, which can occur via digital means. The act provide that (1) A person who sexually abuse or sexually exploits a child in any manner not already mentioned under this part of this Act commits an offence. (2) A person who commits an offence under subsection (1) of this section is liable on conviction to imprisonment for a term of fourteen years.[41] When interpreted together with the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the Child Rights Act serves as a protective legal base for prosecuting online violations against children. The Act thus plays a crucial role in the legal framework for combating cyberbullying in Nigeria, especially when the victim is a minor, and helps in guiding law enforcement and judicial interpretation of children's rights in the digital space.

6.0 INTERNATIONAL LEGAL INSTRUMENTS ON CYBERBULLYING

In reality, the transnational nature of cybercrime and the difficulty in identifying the perpetrator of the place of the crime's commission have created several obstacles and challenges for law enforcement authorities around the world in relation to the obtaining of cross- border evidence and extradition of criminals. Thus, the effective, rapid and well-functioning international cooperation between states on criminal states on criminal matters is essential in enhancing the investigation and prosecution proceedings of cybercrime that is facilitated globally and has negative consequences in different states.

[39] B. Akeusola, 'Social Media and the Incidence of Cyberbullying in Nigeria: Implications for Creating a Safer Online Environment' *Al-Ijtima'i*: *International Journal of Government* and *Social Science* [2023] (9)(1) 99–117

[40] Federal Republic of Nigeria, *Child Rights Act* [2003], s.11

[41] Federal Republic of Nigeria, *Child Rights Act* [2003], s.32(1), (2)

6.1 The Council on Europe's Convention on Cybercrime (Budapest Convention, 2001)

The convention on cybercrime, also known as the Budapest convention on cybercrime or the Budapest convention, is the first international treaty seeking to address internet and computer crime (cybercrime) harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.[42] It was adopted in 2001 by the council of Europe. Although cyberbullying is not expressly mentioned in the convention, its provisions form a foundational international legal framework for addressing various forms of online misconduct, including acts commonly associated with cyberbullying such as cyber stalking, threats, data breaches and online defamation. The convention seeks to harmonize national laws related to cybercrime, improve investigative procedures, and enhance international cooperation in the prosecution of cyber related offenses.

6.2 The United Nations Convention on the Rights of the Child (1989)

The United Nations Convention on the Rights of the Child 1989 (UNCRC) stresses the importance of children's rights and covers four broad areas: survival rights, development rights, protection rights and participation rights. Article 19 of the Convention addresses all forms of violence against children. It considers that violence includes instances where someone attacks a person's mental state as well as physical attacks. In view of this, verbal abuse and intimidation are considered forms of violence. It emphasizes that State Parties must have proper laws in place to prohibit violence, but it also requires states to implement administrative, social and educational measures to protect children.

Article 19 does not stand in isolation and for it to be effective, other Convention rights must also be respected. As well as being protected from violence, Article 19 of the UNCRC says children and young people should be kept safe from all forms of exploitation, sexual abuse, neglect, exposure to accidents, and violent images. Although bullying, including cyberbullying, is not specifically mentioned, it does breach a number of the articles in the Convention. This is further emphasized under the responsibilities of adults to protect and safeguard children and young people from bullying behavior so they may develop, participate in society and lead an assured and contented life. [43]

7.0 CASE LAWS AND REAL- LIFE EXAMPLES OF CYBERBULLYING

In Solomon Okedara v. Attorney General of the Federation, the appellant, Solomon Okedara a Nigerian legal practitioner challenged the constitutionality of Section 24(1) of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. He argued that the provision was vague, overbroad, and lacked clear definitions for terms like "grossly offensive," "obscene," "menacing," and "annoyance." He contended that this vagueness made it possible for legitimate expressions, such as political criticism or artistic content, to be criminalized, thereby violating freedom of expression. Okedara further asserted that the section disproportionately restricted constitutional rights and could be abused by powerful individuals to silence dissent. He argued that criminal laws

[42] Council of Europe, 'Convention on Cybercrime' *European Treaty Series* No. 185, Budapest, 23 November 2001
[43] United Nations, 'Article 17 – Access to Appropriate Information' *Convention on the Rights of the Child* [1989] adopted by General Assembly Resolution 44/25 of 20 November 1989, entered into force 2 September 1990

must be precise and explicit to be valid and enforceable under a democratic constitution. The court, however, held that the National Assembly has the authority to enact laws that are reasonably justifiable in a democratic society, even if they place certain restrictions on fundamental rights. The court found that the language of Section 24(1) which provide that Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or he knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent commits an offence under this Act' was clear enough for legal enforcement and did not infringe on free speech unjustifiably. The appeal was consequently dismissed, and the Cybercrime Act was upheld as constitutional.[44]

In Eniola Badmus v.Okoye Blessing Nwakaego a landmark ruling on August 2, 2023, the Federal High Court in Lagos convicted TikTok user Okoye Blessing Nwakaego for cyberstalking and defaming Nollywood actress Eniola Badmus. The court found that between December 2022 and July 2023, Nwakaego, in collaboration with an accomplice named Chimabia (currently at large), disseminated false and offensive content about Badmus via TikTok and other social media platforms. Nwakaego alleged that Badmus was involved in introducing young Nigerian girls to men, a claim that went viral and severely tarnished the actress's reputation. The defamatory video garnered over three million views online.

During the investigation, Nwakaego confessed that she was offered ₦200,000 by a friend, Fortune Ibe, to produce and share the defamatory content. She expressed remorse, stating that financial desperation led her to commit the act. Justice Nicholas Oweibo sentenced Nwakaego to three years imprisonment, with an option to pay a fine of ₦150,000. The conviction was based on violations of Sections 24(1)(b), 24(2)(a)(c), and 27 of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.[45]

8.0 LEGAL REMEDIES AVAILABLE TO VICTIMS OF CYBERBULLLYING IN NIGERIA

Victims of cyberbullying in Nigeria can seek redress through civil remedies by filing suits against the perpetrators for harm caused by the bullying behavior. While Nigeria currently lacks a distinct tort dedicated solely to cyberbullying, victims can rely on established tort principle's such as the intentional infliction of emotional distress, negligence and invasion of privacy. These torts provide a legal basis for claiming compensation for psychological trauma, anxiety and humiliation resulting from cyberbullying.[46] For example, in Ejike v. Obi[47]the Lagos High Court granted an

[44] Okedara S. v. Attorney General of the Federation (2017) Suit No. FHC/ABJ/CS/263/2016. Unreported.
Cited in: Atoyebi O. & Falade. (2020) 'The Constitutionality of Section 24 of the Cybercrimes Act 2015 in Nigeria: A Critical Analysis of Okedara v AGF', Nigerian Bar Journal, 54-57.
[45] Eniola Badmus v Okoye Blessing Nwakaego Sit No. FHC/L/CS/2023 (Unreported) Cited in: Azeez I. (2023). 'Court's Judgment on TikToker Cyberstalking Case Against Eniola Badmus: A Step Towards Ensuring Online Safety', The Nigerian Lawyer, 2 August 2023.
[46]R. Chesney and D. Citron, 'Deepfakes and the Threats to truth' *California Law Review*,(2019) (107) (7) 1753-1820.
[47] *Ejike v Obi* (2022) 4 NWLR (Pt. 1855) 120.

interim injunction restraining the respondent from further contacting or publishing derogatory content about the applicant on social media, recognizing the mental and reputational harm inflicted through persistent cyber harassment. This case sets a precedent for how civil injunctions can be used effectively to halt ongoing cyberbullying.

Monetary compensation is another core civil remedy. Victims may be awarded damages for medical or therapy expenses, lost income due to emotional breakdown, or other demonstrable losses. In Ibrahim v. Yusuf [48] although not a cyberbullying case per se, the Court of Appeal affirmed the principle that emotional and psychological suffering, where proven, can ground an award of general damages. Injunctive relief remains one of the most effective remedies. A court may order the removal of harmful posts, bar the perpetrator from further online contact, or issue restraining orders to ensure the victim's protection. These measures are especially important in cases involving minors, women, or vulnerable groups who are disproportionately affected by online harassment

However, challenges exist in enforcement, particularly due to difficulties in tracing anonymous accounts and the limited digital forensic capacity of civil courts. Nevertheless, where perpetrators are identified, civil suits remain a strong deterrent, offering victims a path to justice without engaging in protracted criminal proceedings. Civil remedies are therefore crucial in the fight against cyberbullying in Nigeria. They offer victims not just restitution but also legal recognition of their suffering, helping to affirm the right to digital safety and human dignity.[49]

In extreme cases, cyberbullying may rise to the level of a criminal offence under Nigerian law. Acts that involve threats of violence, persistent harassment, or dissemination of explicit content without consent can trigger the applications of statutes such as the Cybercrimes Act 2015. Under sections [50]such as section 24 of the Act, perpetrators may be subject to imprisonment, fines, or both depending on the severity of the offence, criminal prosecution may also result in community service, restraining orders, or mandatory counselling for offenders, particularly where minors are involved. However, one of the primary limitations of criminal prosecution is the higher burden of proof and it lies on the prosecution.[51]

In certain cases, Alternative Dispute Resolution (ADR) mechanisms such as mediation, conciliation, and arbitration offer practical pathways for resolving cyberbullying disputes outside court system. ADR allows for faster, cost effective, and confidential resolution. Mediation, in particular can promote healing and mutual understanding where the disputes arises from a breakdown in personal or social relationships, in Nigeria the multi door courthouse system have adopted resolving disputes among two conflicting parties.[52]

[48] *Ibrahim v Yusuf* (2019) 6 NWLR (Pt. 1676) 463.
[49]A. Comfort Chinyere, 'Extending the frontiers of remedies for crime victims in Nigeria' NJI Law Journal (2009) (1) 106-116.
[50] United Nations office on Drugs and Crime, *Comprehensive study on Cybercrime (UNODC 2013)* 58.
[51] W. Y. Woodage 'Burdens of Proof, Presumptions and Standards of Proof in Criminal cases' *Mizan Law Review* (2014) (8) (1) 252-270
[52] Eze O.C, 'Alternative Dispute Resolution and the Protection of Minors in online Harassment Cases. (2022) 9 (1) Nigerian Journal of Dispute Resolution 61-75.

9.0 CHALLENGES FACED BY CYBER FORENSIC EXPERT

The role of cyber forensic experts in cyberbullying investigations is both crucial and demanding. Unlike traditional crimes, cyberbullying occurs in digital environments, making it necessary to collect and analyze digital evidence across multiple platforms. The process begins with identifying and securing digital traces left by the perpetrator and extends through deep technical analysis in forensic labs, ultimately culminating in the presentation of findings in court. There is no room for error, as improperly handled digital evidence may be ruled inadmissible.[53]

Cyber forensic experts require a range of specialized tools tailored to the nature of digital abuse. In cases of cyberbullying, this may include retrieving deleted social media messages, authenticating screenshots, identifying IP addresses, analyzing mobile communication apps, and verifying user identities. A standard forensic toolkit should consist of software for data recovery, encryption bypass, log auditing, and metadata analysis. Additionally, hardware imaging tools are used to create bit-stream copies of storage devices to ensure the integrity of original evidence.[54]

One major challenge in cyberbullying cases is the anonymity of perpetrators. Cyberbullies often use fake profiles, anonymous platforms, or Virtual Private Networks (VPNs) to conceal their identity, making traceability a complex task. Even when the bullying occurs on popular platforms like Facebook, WhatsApp, or Instagram, forensic experts may struggle to obtain user data due to platform privacy policies and delays in corporate cooperation.[55]

Proper planning and legal compliance are also critical. Evidence must be collected following strict procedures to avoid tampering or data corruption. This includes cloning data for examination while preserving the original. Given that cyberbullying evidence such as messages, images, or posts can be easily deleted or manipulated, timely acquisition is essential.[56]

Furthermore, technical challenges arise from the fact that digital evidence is stored in bits and bytes, not easily visible or accessible without advanced tools. Social media platforms use end-to-end encryption, which complicates efforts to access communications between the bully and the victim. Even when forensic tools are available, experts may lack access to updated software or training, especially in under-resourced regions. Additionally, victims' reluctance to report bullying or provide devices for forensic analysis can limit the investigation. Fear of stigma or further harassment discourages cooperation, making it harder for experts to gather a complete digital trail.[57]

In summary, the challenges faced by cyber forensic experts in cyberbullying cases include:

---

[53] E. Casey, 'Digital Evidence and Computer Crime: Forensic Science, Computers, and the internet' *Academic Press,*(2011) 101-144.

[54] J. Sammons 'The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress Publishing, 59.

[55] Ayodeji A. (2021). 'Challenges in the investigation and prosecution of cyberbullying in Nigeria' (2021) Journal of Law and Digital Society 35-48.

[56] K. Shivashankar, 'Digital Evidence in Cyber Bullying Cases: Emerging Challenges' (2019) 12 (1) 140-153.

[57] A. Oyetibo,'Victim Silence and its Impact on Cyberbullying Investigations in Nigeria' *Law and Human Rights Review*, 41-52.

- Anonymity and use of fake profiles by perpetrators.
- Difficulty obtaining timely cooperation from social media platforms.
- Technical barriers like encryption and data volatility.
- Legal and ethical concerns in handling personal digital data.
- Limited resources and training.
- Victim reluctance and delayed reporting.

10.0 FINDINGS

This paper reveals several important findings regarding the state of cyberbullying and victim protection in Nigeria. First, it is evident that the country lacks a comprehensive and specific legal definition of cyberbullying. Although the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 criminalizes some related actions, such as cyberstalking and online harassment, it fails to address other prevalent forms of abuse like trolling, doxxing, and the non-consensual sharing of intimate images. This legislative gap makes it difficult to prosecute offenders and leaves many victims without adequate legal remedies.

Furthermore, the institutions responsible for enforcing cybercrime laws, including the Nigerian Police Force, the National Information Technology Development Agency (NITDA), and the Nigerian Communications Commission (NCC), face significant challenges. These include inadequate training, poor technical infrastructure, and limited coordination. As a result, many cases of cyberbullying go unreported or unresolved.

The study also found that public awareness of cyberbullying laws and digital rights is low, particularly among young people who are most vulnerable to online abuse. Victim support systems such as legal aid, counseling, and anonymous reporting platforms are either absent or poorly structured. Additionally, while Nigeria has ratified international instruments such as the Budapest Convention and the United Nations Convention on the Rights of the Child (UNCRC), these treaties have not been fully implemented into domestic law, reducing their effectiveness in practice.

11.0 CONCLUSION

This paper has provided a comprehensive examination of the legal and institutional frameworks governing cyberbullying and victim protection in Nigeria. Guided by its objectives, the study critically explored the causes and consequences of cyberbullying, the existing legal instruments addressing it, the institutions responsible for enforcement, and the adequacy of victim protection mechanisms.

It is evident from the findings that cyberbullying is no longer a marginal or occasional issue it has evolved into a widespread digital menace, especially among Nigerian youths, amplified by the rise of smartphones, anonymity on social media platforms, and low digital literacy. The psychological, emotional, and social harm suffered by victims is real and, in some instances, irreversible. Despite the provisions of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and other related laws, Nigeria still lacks a comprehensive legal framework that directly defines and addresses

cyberbullying in its various forms such as trolling, doxxing, outing, impersonation, and online shaming. Section 24 of the Act, which addresses cyberstalking and offensive communication, offers limited protection and has proven inadequate in practice.

Furthermore, enforcement remains weak due to the limited technical capacity, poor coordination, and underfunding of institutions such as the Nigerian Communications Commission (NCC), the National Information Technology Development Agency (NITDA), Nigerian Data Protection Regulation (NDPR), The Nigeria Police Force. Victims are often left without adequate support due to the absence of specialized reporting channels and legal aid.

This study also revealed the critical gap between legal provisions and public awareness. Many Nigerians are not aware of their rights online or how to seek redress when cyberbullied. Meanwhile, international legal instruments ratified by Nigeria, including the UN Convention on the Rights of the Child and the Budapest Convention, have not been fully domesticated, thereby limiting their enforcement potential.

It must be emphasized that cyberbullying is not simply a technological problem it is a legal, institutional, and societal challenge. Addressing it requires a holistic approach that includes legislative reform, institutional strengthening, digital education, and the active involvement of tech platforms in safeguarding users.

In summary, the current Nigerian legal and institutional framework falls short in protecting victims of cyberbullying and deterring perpetrators. Urgent reform is needed to introduce clear legal definitions, enhance enforcement mechanisms, provide victim-centered remedies, and raise public awareness. Only then can Nigeria build a robust digital rights regime that ensures safety, dignity, and accountability in its evolving online space.

12.0 RECOMMENDATIONS

Based on the above findings, this paper puts forward several recommendations to improve the legal and institutional response to cyberbullying in Nigeria. First, there is an urgent need to amend existing laws or introduce a standalone Cyberbullying Prohibition Act. Such legislation should clearly define cyberbullying, categorize its forms, and provide appropriate penalties for each offence.

Second, the enforcement capacity of institutions must be strengthened. Law enforcement officers, especially those in cybercrime units, should be trained in handling digital evidence and responding sensitively to victims. Agencies like the NCC and NITDA should also be empowered with better tools and resources to monitor and regulate online spaces.

Third, public awareness campaigns are essential. These should aim at educating the citizens, especially youths, on what constitutes cyberbullying, their rights under the law, and how to report abuse. Digital literacy should be incorporated into school curricula at all levels to promote safer online behavior.

Fourth, comprehensive victim support mechanisms should be established. These may include toll-free helplines, digital reporting platforms, legal aid services, and access to mental health support.

Government agencies, in collaboration with NGOs and educational institutions, should create safe spaces for victims to report incidents without fear of stigma or retaliation.

Fifth, Nigeria should fully domesticate and enforce international conventions like the Budapest Convention and the UNCRC. This would align Nigeria's legal framework with global best practices and enable stronger cross-border cooperation in cybercrime investigations.

Finally, technology companies and social media platforms operating within Nigeria must be held accountable. Regulatory frameworks should be introduced requiring these platforms to respond promptly to cyberbullying complaints, take down harmful content, and cooperate with local law enforcement agencies.