TITLE PAGE

CYBERBULLYING AND ONLINE HARRASSMENT: A CRITICAL EXAMINATION OF ICT LAWS AND POLICIES.

DECLARATION

I, Cherish Arongs, hereby solemnly declare that this research work, titled **Cyberbullying and Online Harassment: A Critical Analysis of ICT Laws and Policies**, submitted in partial fulfilment of the requirements for the award of LL. B, is an original and authentic production of my intellectual endeavors.

I attest that:

1. This research work has not been previously submitted, published, or disseminated in any form.

2. All sources utilized in this research have been properly acknowledged, cited, and referenced in accordance with established academic conventions.

3. This work does not infringe upon any copyright, patent, trademark, or other intellectual property rights.

4. This research was conducted in compliance with applicable laws, regulations, and ethical standards.
research.

Date:_____
Name:_____
Matric Number: _____

CERTIFICATION

This is to certify that this long essay titled **"Cyberbullying and Online Harassment: A Critical Analysis of ICT Laws and Policies"** has been assessed and approved by the Undergraduate Studies Committee of the Faculty of Law, Alex Ekwueme Federal University, Ndufu Alike Ikwo as an original work carried out by **Arongs Cherish Akahema** with registration number **2020/LW/23543** in the Faculty of Law, Alex Ekwueme Federal University, Ndufu Alike Ikwo, under the guidance and supervision of Anoke Uwadiegwu (Esq).

_____ _____

Arongs Cherish Akahema **Date**

(Student)

_____ _____

Anoke Uwadiegwu **Date**

(Supervisor)

_____ _____

Dr Kelechi Onyegbule **Date**

(Project Cordinator)

_____ _____

Proff. Eseni Azu Udu **Date**

(Dean, Faculty of Law)

_____ _____

(**External Examiner**) **Date**

ACKNOWLEDGEMENT

Firstly, I acknowledge the Almighty and Ever Faithful God for His grace and mercies upon my life.

I extend my appreciation to the Dean, Faculty of Law, Alex Ekwueme Federal University Ndufu Alike Ikwo, Ebonyi State Proff. Eseni Azu Udu who is always ready to ensure that his students, the faculty, and the University at large soar higher than the eagles.

I further extend my profound gratitude to the Pioneer Dean Faculty of Law, Dr. Onyekachi Eni who tirelessly worked to instill discipline in us, to Dr. O. T. Ezeh who has been like a mother to us, and to all my amiable and hardworking lecturers (Dr. Ituma, Dr. Amadi, Dr. Kelechi, Barr. Charity, Barr. Ekechi, Barr. Nweze, Barr. Paschal, Barr. Nwambam, Barr. Chukwudifu, Barr. Awoke).

This section would be incomplete if I fail to specially appreciate Barr. Uwadiegwu Anoke, my supervisor. Thank you for your advice, corrections and guidiance throughout this research work, Sir.

For the sacrifices, the love, the care, the advice and encouragements, I express my deepest gratitude to my loving parents, Mr. Emmanuel (EAU) and Eld. Mrs. Glory Arongs. I do not take your sacrifices for granted, my sweet people. I also appreciate my big brothers, Reverend Regal and Barr. Best Arongs. Your little contributions and efforts were recognized and cherished.

Last but not the least, I want to thank me. I want to thank me for believing in me. I want to thank me for doing all this hard work. I want to thank me for having no days off. I want to thank me for never quitting. I want to thank me for always being a giver and trying to give more than I receive. I want to thank me for trying to do more right than wrong. I want to thank me for just being me at all times.

DEDICATION

To the Almighty God who makes things right in his time.

And to my dad (Mr. Emmanuel), whose sacrifices and words of encouragement have served as a pillar that holds me when I am about to collapse.

TABLE OF CASES

TABLE OF STATUTES

LIST OF ABBREVIATIONS

ICT	Information and Communication Technologies
LGBTQ	Lesbian, Gay, Bisexual, Transgender, Queer
UK	United Kingdom
US	United States
IMS	Information Management System
UNICEF	United Nations Children's Fund
NGOs	Non-Governmental Oraganizations
NCC	Nigerian Communications Commission
NCPWD	National Centre for Promotion of Employment for Disabled People
NPF	Nigeria Police Force
EFCC	Economic and Financial Crimes Commission

TABLE OF CONTENTS

ABSTRACT

The advent of the internet and social media has transformed the way people interact and communicate. However, this increased connectivity has also given rise to cyberbullying and online harassment, which can have devastating consequences on individuals, particularly vulnerable groups such as children and women. Nigeria, with its growing online presence, is not immune to these problems. Despite the growing concern about cyberbullying and online harassment, there is a dearth of research on the effectiveness of existing ICT laws and policies in Nigeria in addressing these issues. This study aims to bridge this knowledge gap by critically examining the current ICT laws and policies in Nigeria and their implications for combating cyberbullying and online harassment. The study reveals that while Nigeria has made some efforts to address cyberbullying and online harassment through legislation and policy initiatives, there are significant gaps and challenges in the existing framework. The study highlights issues of inadequate regulation, lack of enforcement, and limited awareness and education about cyberbullying and online harassment. This study employs a doctrinal research methodology, involving a critical analysis of existing ICT laws and policies in Nigeria, as well as online literatures, newspapers, magazines and internet materials. The study concludes that Nigeria's existing ICT laws and policies are inadequate to effectively address the growing problem of cyberbullying and online harassment. The study highlights the need for a more comprehensive and nuanced approach to addressing these issues, including strengthened legislation, improved enforcement, and increased awareness and education. The study recommends the following: (a) review and amendment of existing ICT laws and policies to specifically address cyberbullying and online harassment (b) establishment of a national cyberbullying and online harassment reporting mechanism (c) development of public awareness and education campaigns to promote online safety and digital literacy; and (d) strengthening of law enforcement capacity to investigate and prosecute cyberbullying and online harassment cases.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

The swift evolution of Information and Communication Technologies (ICT) has transformed the way we communicate, interact, and share information. The growth of social media, online platforms and digital tools has facilitated unique level of connectivity, personal expression, and collaboration. However, this digital landscape has given opportunities to new forms of aggression, harassment and bullying notably cyberbullying and online harassment. These has led to grievous and severe effects and consequences on persons, communities and the society at large as it affects mental health, social life, and even physical safety. Cyberbullying has ushered in a new area of cruelty and elevated the spread of hate and hurt exponentially. In previous generations, we were limited in our ability to spread information.[1]

The anonymity and reach of the internet can embolden persons to display behaviour which they might not display in person, leading to online abuse, harassment and hate speech. Cyberbullying involves the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behavior, aimed at scaring, angering, or shaming those who are targeted. Examples include:

-Spreading lies about or posting embarrassing photos or videos of someone on social media

-Sending hurtful, abusive or threatening messages, images or videos via messaging platforms

[1] Let's talk about Cyberbullying: What is it and what can we do about it? Available at < https://thescreentimeconsultant.com/blog/lets-talk-about-cyberbullying > accessed 23 April 2025.

-Impersonating someone and sending mean messages to others on their behalf or through fake accounts.

-Engaging in sexual harassment or bullying using generative AI tools.[2]

The impact can be particularly pronounced for vulnerable populations, such as children, adolescents, and marginalized groups, who face increased risks of online victimization. Despite the increasing concern and awareness about Cyberbullying and online harassment, the efficacy of existing ICT laws in tackling these issues remains a subject of critical examination. Many countries have enacted laws and rules targeted at combating online abuse but the variation of digital platforms, together with the unlimited scope of the internet present major difficulties to accountability and enforcement. There is also the issue of regulating online content and protecting the freedom of expression.

This work aims to explore the intersection of law, social behavior, technology, analyzing the strengths and limitations of current ICT laws in protecting individuals from online abuse and harassment. By examining the legal frameworks, enforcement mechanisms, and social implications of cyberbullying and online harassment. It provides insights into the complexities of regulating online interactions and safeguarding digital citizens. The research will investigate the experiences of victims, the responses of online platforms and authorities, and the impact of ICT laws on online behaviour, with a view to identify best practices and areas for improvement.

Through a critical analysis/examination of ICT laws and their uses, this project seeks to contribute to the development of an improved methodology for mitigating cyberbullying and online harassment. By highlighting the complexities of online aggression, and the role of law in

[2] Cyberbullying: What is it and how to stop it. Available at < https://www.unicef.org > accessed 23 April 2025.

addressing it, this research aims to inform policy debates, guide practices and ultimately enhance the safety and well-being of individuals in the digital age.

1.2 Statement of the problem

The emergence of the digital age has redefined communication, access to information globally and social interaction. In Nigeria, the expansion of internet usage, mobile technology, and high engagements of social media platforms like Facebook, Twitter (X), Instagram, TikTok, and WhatsApp has markedly transformed how individuals engage with one another. While this digital development has created positive opportunities for education, commerce, and civic participation, it has also triggered undesirable consequences chief amongst them being cyberbullying and online harassment.

Cyberbullying and online harassment refers to the use of digital technologies to threaten, stalk, defame, harass, or otherwise abuse individuals through persistent and malicious behavior. Victims experience a range of harmful conduct including name-calling, hate speech, character assassination, doxxing (unauthorized sharing of personal information), revenge pornography, cyberstalking, and coordinated online attacks. These kinds of cyber violence often leads to severe psychological and emotional trauma, social isolation, reputational damage, depression, and, in some extreme cases, suicidal thoughts or suicide.

A number of persons including women, children, teenagers, members of the LGBTQ+ community, and public figures are among the most commonly targeted groups.

In Nigeria, these issues are becoming more noticeable, yet they remain inadequately dealt with by existing legal and institutional mechanisms. Although the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 was enacted to criminalize and regulate offenses committed via

digital platforms, its provisions regarding cyberbullying and online harassment are limited in scope and effectiveness. The law primarily focuses on financial crimes, hacking, and cyberterrorism, with ambiguous definitions and insufficient legal protections for victims of non-financial forms of online abuse. In many cases, the enforcement of these laws has been unpredictable or hampered by a lack of technical expertise, limited resources within law enforcement agencies, and lack of public knowledge about digital rights.

Additionally, there exists a gap in synergy between the law, policy implementation, and public education. Victims are often reluctant to report cases due to fears of stigmatization, mistrust in the justice system, or lack of awareness about legal recourse. Furthermore, even when complaints are lodged, the legal process is often delayed, cumbersome, and affected by systemic institutional challenges. The absence of clear reporting procedures, digital forensic tools, and specialized personnels significantly hinders the timely and effective adjudication of such matters.

There is also a visible gap between Nigeria's ICT legal framework and international standards or best practices, such as those outlined by the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), United Nations and human rights-based approaches to cyber governance. The absence of thorough legislation that explicitly addresses cyberbullying as a standalone offense—combined with poor enforcement and the digital illiteracy of many citizens—raises serious concerns about the capacity of Nigeria's legal system to protect individuals in the online space.

This situation underscores the need for a critical examination of Nigeria's ICT laws, with a focus on identifying gaps, challenges, and opportunities for reform in addressing cyberbullying and online harassment. Without legal interventions, institutional strengthening, and widespread

public sensitization, the problem will likely escalate, eroding trust in digital platforms and compromising the safety and dignity of Nigerian citizens online.
The research questions that will guide this analysis include:

1. What is Cyberbullying and online harassment?

2. How effective are ICT laws in addressing Cyberbullying and Online Harassment in Nigeria?

3. What is the scope of Nigerian legal and regulatory framework in protecting victims of Cyberbullying and Online Harassment?

4. Does Nigeria comply with with international practices in combating Cyberbullying and how well does it do it?

1.3 Aims and objectives of the study

The main aim of the study is to critically examine the adequacy, effectiveness, and enforcement of Nigeria's ICT laws in addressing cyberbullying and online harassment, while identifying legal gaps and proposing reforms to ensure better protection of victims and accountability for offenders. The other objectives are;

a. To define and contextualize cyberbullying and online harassment.

b. To critically examine the effectiveness of Nigeria's ICT laws (e.g., the Cybercrimes (Prohibition, Prevention, etc.) Act 2015) in addressing cyberbullying and online harassment and analyze the scope to which Nigerian legal and regulatory frameworks protect victims of online abuse, particularly on social media and digital platforms.

c. To propose legal reforms or policy recommendations that can enhance the Nigerian legal system's response to cyberbullying and online harassment.

f. To compare Nigeria's legal framework with those of other jurisdictions (e.g., UK, South Africa, USA) to identify best practices and lessons Nigeria can adopt. To gauge public awareness and legal literacy around rights, remedies, and reporting mechanisms for online abuse.

1.4 Scope and Limitations of the study

This study aims at examining the legal framework governing cyberbullying and online harassment in Nigeria, with emphasis on the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the 1999 Constitution (as amended), and other relevant ICT-related laws and regulatory policies.

The research intends to judiciously assess the level to which these laws deal with cyberbullying and online harassment, identify existing legal gaps, and propose reform recommendations.

This study also addresses:

-A review of relevant case laws, both Nigerian and international.

-An analysis of the enforcement mechanisms and the challenges faced by law enforcement agencies and victims.

-A comparative analysis with select foreign jurisdictions (e.g., UK, US, India) to highlight global best practices and their relevance to Nigeria.

The study has a number of limitations including:

-The research is limited to Nigerian laws and institutions. Though it cites international practices for comparison, it does not exhaustively explore international treaties or the laws of all countries.

-The study is primarily doctrinal and does not involve primary data collection such as interviews or surveys with victims, legal practitioners, or enforcement officers as it relies on secondary data sources like existing literature, case laws, and reports from law enforcement agencies.

-The study emphasizes legal and institutional analysis and does not extensively delve into the psychological or sociological dimensions of cyberbullying and online harassment.

-The dynamic nature of digital technology and online platforms means that a number of regulatory responses may become outdated quickly, limiting the long-term applicability of certain observations.

-Due to inconsistencies in the public availability of cybercrime-related court judgments in Nigeria, some aspects of the judicial response may be underrepresented.

Despite these limitations, the study provides a critical and relevant examination of Nigeria's current legal framework in dealing with cyberbullying and online harassment and provides practical recommendations for improvement.

1.5 Significance of the study

This study has both theoretical and practical significance. Theoretically, this study contributes to the existing literature on cyberbullying and cybercrime laws in Nigeria by providing a critical analysis of the cybercrime Act and other exiisting laws.

This analysis sheds light on cyberbullying and online harassment, the weakness of the Cybercrime Act in exhaustively addressing Cyberbullying. The study will also help to deepen

our understanding of the legal framework for combating cyberbullying in and outside the country and sheds light on the effectiveness of the current legislation on addressing online harassment. Practically, the findings of this study can be used by other researchers, policymakers, law enforcement agencies, and other stakeholders to improve and implement cyberbullying and online harassment laws and enhance cybersecurity measures in Nigeria.

1.6 Research methodology

This study seeks to evaluate the effectiveness of Cyberbullying laws in addressing the growing threats of Cyberbullying and online harassment in Nigeria. To accomplish this, the study will make use of the doctrinal approach in analyzing Cyberbullying laws such as the Cybercrime (Prohibition, Prevention, etc.) Act 2015 in Nigeria. This is because the doctrinal research is the most popular method used by legal researchers.

The library-based study seems to determine what the law is in a certain circumstance. It concentrates on the analysis of legal rules and principles, including how it was formed and applied. As is generally known, this research is completely theoretical, consisting of simple research targeted at locating a single declaration of the law or legal analysis.

Hence, the goal of this methodology is to carry out specific investigations, in order to discover specific bits of information. The reason for adoption of this research is to examine and interpret existing legal frameworks on cyberbullying and online harassment in Nigeria. It emphasizes the statutes, case laws, and legal commentaries, especially the Cybercrimes Act 2015. This method is appropriate for recognizing legal gaps and inconsistencies. It also allows for comparison with international standards. Doctrinal research is appropriate for legal studies as it relies on authoritative sources without requiring fieldwork.

CHAPTER TWO

CONCEPTUAL CLARIFICATIONS THEORETICAL FOUNDATION AND LITERATURE REVIEW

2.1 CONCEPTUAL CLARIFICATIONS

At this juncture, we will be considering the concept of bullying, cyberbullying, the history and evolution of cyberbullying, online harassment, the convergence and divergence between Cyberbullying, Online harassment, and other forms of violence and harassment and the impact of Cyberbullying and Online harassment on individuals and the society at large.

2.1.1 The Concept of Bullying

There is a widely reported story of one Amanda Michelle Todd[3], a Canadian teenager who went through persistent bullying as she was harassed both offline and online, which led to serious emotional distress and finally suicide in 2012. A month before her death, she posted a self-made video on YouTube. She used a series of flashcards to tell her story of online sexual exploitation, and the emotional distress and verbal and physical abuse that followed her in real life.[4]

There is another prominent story of Tyler Clementi, who was an American student who faced severe cyberbullying from his roommate who secretly recorded his intimate encounter and live-streamed it online, leading to widespread harassment and ridicule. These and many other stories have prompted widespread concern and raised many questions as to what act actually constitutes bullying. Bullying is the repetitive, intentional hurting of one person or group by another person

[3] November 27 1966--October 10 2012.

[4] The Canadian Encyclopedia. Available at <https://www.thecanadianencyclopedia.ca> accessed on

or group, where the relationship involves an imbalance of power. Bullying, can be physical, verbal or psychological. It can happen face-to-face or online.

According to Eve, Lori and Katherine, researchers have identified four main types of bullying: physical, verbal, relational, and cyber. Physical bullying is characterized by physical acts of aggression, such as hitting, punching, or pushing. Relational bullying, also referred to as social exclusion bullying, is characterized by rumor spreading and purposefully leaving others out of activities or interactions, or friendship withholding (Crick & Grotpeter 1995). Verbal bullying is characterized by spoken aggressions, such as name calling and teasing (Bauman & Del Rio 2006). Cyberbullying is peer aggression committed using technology such as text messages, emails, or social networking sites (Butler et al. 2009).[5]

Bullying is an form of consistent threats or harm which may be physically or online which causes physical or emotional trauma to the victim(s). It is when someone is being hurt on purpose several times by another person through words or actions.

2.1.2 Cyberbullying

Cyberbullying has emerged as a pressing global issue, transcending geographical boundaries and impacting individuals of all ages, particularly minors. In the digital age, where connectivity is ubiquitous, cyberbullying represents a dark facet of the online world. Unlike traditional forms of bullying, which may be confined to physical spaces like schools or neighborhoods, cyberbullying

[5] Eve M. Brank, Lori A. Hoetger, and Katherine P. Hazen, 'Bullying'. Annual Review of Law and Social Science 213-230. [2012] (8)(1)

extends its reach into the virtual realm, where perpetrators can harass, intimidate, or harm their victims through electronic means (Hinduja & Patchin, 2015).[6]

In Nigeria, there's no legislation or act that clearly defines Cyberbullying. However, the **Cybercrime Act 2015** uses Cyberstalking interchangeably with cyberbullying. It made an attempt to define cyberstalking. It may be seen to be the act of causing knowingly or intentionally sending a message or matter. Cyberbullying was first defined by the Merriam-Webster Dictionary as "the electronic posting of mean-spirited messages about a person (such as a student) often done anonymously".

The Law Dictionary defines Cyberbullying as the willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices. Examples of cyberbullying may include repeated cruel texts and instant messages (IMS), posting private or embarrassing photos, creating social media groups just to target one individual or group, hacking into social media or gaming accounts, spreading gossip and rumors online, cyberbullying is bullying which occurs online. It involves persistent and deliberate harassment that causes harm to the particular individual.

The term Cyberbullying is used broadly, both in colloquial and formal use. First, coined in 1999, there's no general consensus on a definition, although different versions usually include the use

[6] James P. Friday & Mary P. Soroaye, 'CYBERBULLYING LAWS IN NIGERIA: SAFEGUARDING MINORS' RIGHTS IN THE DIGITAL AGE' Available at: <https://www.researchgate.net/publication/379655306> accessed June 2, 2025.

of digital technology to inflict harm repeatedly or to bully. In 2006, **Patchin** an **Hinduja** defined cyberbullying as willful and repeated harm inflicted through the use of computers, cell phones or other electronic devices. **Kowalski et al** defined it in 2014 as the use of electronic communications technology to bully others.[7]

In **Smith's** words, "Cyberbullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact, repeatedly and over time, against a victim who cannot easily defend themselves.

According to **UNICEF**, it can be seen as bullying with the use of digital technologies. It can take place on social media, messaging platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted.

The most common places where cyberbullying occurs are:

-Social Media, such as Facebook, Instagram, Snapchat, and Tik Tok

-Text messaging and messaging apps on mobile or tablet devices

-Instant messaging, direct messaging, and online chatting over the internet

-Online forums, chat rooms, and message boards, such as Reddit

-Email

-Online gaming communities.[8]

---

[7] Available at < https://publications.aap.org/pediatrics/article/140/Supplement_2/S148/34183/Defining-Cyberbullying >

[8] Available at < https://www.stopbullying.gov/cyberbullying/what-is-it >

Psychologist may define it as a form of psychological abuse where perpetrators make use technology to exert control, inflict emotional pain, or socially isolate the victim, which often leads to anxiety, depression, or reduced self-esteem. Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. It can include sending, posting, or sharing negative, harmful, false, or mean content about someone else, including sharing personal or private information.[9]

Cyberbullying commonly involves a power imbalance between the bully and the victim.The bully usually has more control or influence online. It can lead to feelings of shame, anxiety, and isolation, and can negatively impact mental health and well-being. Cyberbullying is often associated with teens or students. However, everyone can be a victim of cyberbullying including children, adults, men, women, poor, wealthy etc. Cyberbullying can take place between students, colleagues at work, neighbours, friends, family relatives, strangers and a list of others.

Cyberbullying refers to the use of electronic communication to threaten or harass an individual, which often involves repeated, intentional acts that cause emotional harm to the victim. Laws vary by state, but many define it as electronic harassment that includes threats, humiliation, or stalking.

Cyberbullying has been defined as individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others.[10] Cyberbullying is a relatively new medium through which bullying occurs (e.g., chat rooms, text messages). Cyberbullying has been defined as an individual or a group willfully using information and

[9] United Nations Educatiional, Scientific and Cultural Organization (UNESCO)

[10] Computers in Human Behavior, 2010.

communication involving electronic technologies to facilitate deliberate and repeated harassment or threat to another individual or group by sending or posting cruel text and/or graphics using technological means.

2.1.3 Historical Evolution of Cyberbullying

Long ago, when they was little or no technology, people were only bullied physically, verbally, or socially due to limited internet access. With time, technology began to spread and phones, together with other forms of computers became widely used and the internet became more accessible, people started making use of technology to bully others.

At this point, cyber bullying was not taken seriously as it was ignored, treated as a joke, and was not recognized legally or socially as a significant problem until social media and technology became more widely used and cases of online shaming, impersonation, threats, and trolling, especially targeting children, women, celebrities, and activists kept increasing. The growing prevalence of cyberbullying, especially against public figures like celebrities and activists, spurred NGOs and youth groups to begin advocating for digital safety awareness. At this point, victims experienced online trolling, character attacks hate speech and few cases of extortion, revenge porn and cyber-harassment which began to gain media attention.

The first-time cyberbullying appeared in the English language was in 1998. Cyberbullying was defined by the Merriam-Webster Dictionary as "the electronic posting of mean-spirited messages

about a person (such as a student) often done anonymously." The definition has evolved as the Internet has evolved.[11]

Consequently, cyberbullying began to gain legal attention leading to the establishment of some laws including the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 which was passed into law by President Goodluck Jonathan. Though the Act didn't clearly define Cyberbullying or state the punishment for bullies, the Act criminalized cyberstalking, online harassment, and related offenses[12]. It gave law enforcement authority to investigate and prosecute cyberbullying. This marked a turning point, giving Nigeria a legal framework to address cyberbullying and cyber harassment. Around this time, schools and universities began reporting more cases of cyberbullying which led to more National conversations around mental health and online abuse.

Cyberbullying is now a major social issue in Nigeria with more awareness campaigns by NGOs, schools, government bodies and international bodies.

Summarily, Cyberbullying in Nigeria evolved from small-scale insults in the early internet forums to a widespread phenomenon fueled by social media. Today, it affects citizens, students, activists and celebrities. Though they're laws which exist for enforcement and awareness still ongoing.

---

[11] Available at < https://www.southern.k12.oh.us/cyberbullying#:~:text=The%20first%20time%20cyberbullying%20appeared,as%20the%20Internet%20has%20evolved >

[12] Section 24, Cybercrime (Prohibition, Prevention, etc.) Act of 2015.

2.1.4 Understanding the Concept of Online Harassment

Just like Cyberbullying, online harassment does not have a universally acceptable definition and the terms are often used interchangeably. However, online harassment is a broader term that includes doxing, impersonation, cyberbullying, online stalking, revenge porn etc.

The term online harassment refers to utilization of information and communication technologies by an individual or a group to repeatedly inflict harm upon another person. This may encompass issuing threats, causing embarrassment, or inducing humiliation in a virtual environment.[13]

It may also be defined as the use of threats, embarrassment, or humiliation in an online setting. This includes expressions of discriminatory attitudes and beliefs—such as sexism, racism, xenophobia, homophobia, transphobia or ableist prejudices. It also includes online sexual harassment, cyberstalking, and image based sexual abuse or other unwanted online conduct of a sexual nature.[14]

Online harassment can be called cyberaggression, cyberbullying, cyber-harassment, cyberhate, cybervictimization, and deviant online conduct.

Online harassment, also referred to as cyber-harassment or online abuse, refers to a situation in which an individual or group is severely or pervasively targeted through harmful online behaviour that may be for either a short or extended duration, may be perpetrated by either an individual or coordinated by a group of people, and which is aimed at causing severe emotional distress or emotional harm.

---

[13] Available at < https://reportandsupport.ox.ac.uk/support/what-is-online-harassment#:~:text=The%20term%20online%20harassment%20refers,humiliation%20in%20a%20virtual%20environment >

[14] See more at < https://reportandsupport.durham.ac.uk/support/what-is-online-harassment >

It can occur in a variety of forms including:

a. Cyberbullying

b. Cyberstalking

c. Doxing

d. Online impersonation

e. Trolling

Nigeria's primary legal framework for addressing online offences is the Cybercrime (Prohibition, Prevention) Act, 2015 as amended in 2024. It is important to note that the Act does not expressly provide for the offenses of cyberbullying and online harassment rather, they're said to be fixed or classified under cyberstalking.

2.1.5 The Impact of Cyberbullying and Online Harassment on Individuals and the Society

Cyberbullying can have severe negative effects on individuals and the society at large. Its victims lack mental, emotional, and even physical well-being.

Some effects on individuals include;

a. Emotional and Psychological effects:

- Low self-esteem

- Stress and trauma

- Depression and anxiety

- Suicidal thoughts[15]

b. Physical Health Effects:

- Victims may develop headaches, eating disorders, or other stress-related illnesses.

c. Social and Educational Effects:

- Poor academic work performance

-Damage of reputation

-Withdrawal from relationships

Societal effects include;

a. Impact on Youth and Education:

- Leads to digital insecurity

- Increases cases of school violence

b. Breakdown of trust:

- Discourages civic engagement and silences voices

- Creates toxic online where individuals are unable to express themselves.

c. Mental Health Burden on Society:

- Creates a generation of struggling with insecurity and trauma

[15] Amanda Michelle Todd (November 27, 1966--October 10, 2012).

- Increase in mental health cases.

2.2 THEORITICAL FOUNDATION

2.2.1 Theories of Digital Behaviour:

This theory explains cyberbullying as an effect of the unique features of digital spaces including anonimity, permanence and asynchronity which reshapes human behaviour and reduces social expectations.

2.2.2 Anonimity and aggression:

This theory explains Cyberbullying as a product of reduced accountability in anonymous online environment which promotes hostile behaviors and increases harassment.

2.2.3 Social learning theory:

This theory is of the view that people learn behavior through observation, reinforcement and imitation. It is often used to explain why Cyberbullying and online harassment occur and how such behaviors are sustained.

2.2.4 Routine Activities Theory (RAT):

Routine Activities Theory (RAT) offers a robust lens for analyzing cyberbullying and online harassment, especially in Nigeria, as digital activities become more central to daily life. RAT, credited to Cohen and Felson, posits that crime occurs when a motivated offender encounters a suitable target in the absence of a capable guardian (Adeoye et al., 2025). Unlike other theories

focused on psychological or biological causes, RAT emphasizes the environmental and contextual dynamic space, time, and opportunity that allow crime to flourish[16].

Theoretical Expansion and Digital Adaptation

Routine Activities Theory has spread beyond the traditional crime settings to involve digital environments. Researchers like Xiao et al. (2016) and Navarro & Jasinski (2012) have adapted RAT's main elements for online contexts: motivated offenders (those who seek to bully or harass online), suitable targets (including vocal social media users or visible public figures), and the absence of guardianship (like digital literacy or platform moderation). In their studies, online routines such as posting photos, sharing personal updates, or engaging in heated discussions make individuals more susceptible to being targeted. Measures of guardianship, such as browser history checks, website filters, and parental oversight, were shown to lower risks for adolescents[17].

Further research such as Reyns et al. (2011) expands the idea to cyberspace, noting that physical proximity is replaced by networked contact: offenders and victims may never meet in person, but intersect within digital platforms and online communities. The likelihood of victimization increases with time spent online and frequency of exposure to offenders[18].

Local Patterns and Challenges

[16] Miró, F., 'Routine activity theory and its application to crime in cyberspace' (2014). In Cohen, L. E., & Felson, M. 'Crime and Everyday Life: Insight on Routine Activity Theory' (1979).

[17] Navarro, J. N, & Jasinski, J. L, 'Predicting cyberbullying: Routine activity theory' (2012).

[18] Bossler et al., 2012; Hinduja & Patchin, 2008.

For Nigeria, RAT has been instrumental in analyzing patterns of cyberbullying. Federal Polytechnic Ilaro's case studies found that students became heightened targets during campus election periods when their online activities rose, and public attention shifted to social media platforms (Adeoye et al., 2025). Lagos-based influencers have similarly been targeted during major national events or controversies; the lack of both digital guardianship (platform controls and official monitoring) and timely law enforcement responses compounds their vulnerability (Salford Repository, 2020).

Nigeria's rapid internet growth increases exposure to digital offenders. Yet, enforcement and protection lag—law enforcement agencies grapple with both technical limits and capacity challenges, as highlighted in recent research on cybercrime investigation efficacy. Studies show that online proximity—being in common digital spaces where offenders operate—magnifies risk, especially among youth and outspoken individuals (Li et al., 2020).

There have been cases involving students activities, musicians, or political figures often emerging in public debate, with waves of organized harassment during key events. For instance, during the EndSARS protests and SUG elections in some universities, increased posting and engagement on Twitter and Instagram led to heightened instances of cyberbullying and threats. Many incidents went unpunished due to weak digital guardianship where platform policies were insufficient and local law enforcement responses slow or non-existent (Salford Repository, 2020).

Implications and Prevention Strategies

Researchers advocate several prevention measures drawn from RAT:

-Stronger digital guardianship, such as real-time AI monitoring and proactive moderation.

-Community digital literacy programs to help Nigerians recognize online risks and respond appropriately.

-Law enforcement and policy intervention, including implementation of the Cybercrime Act, to bolster institutional responses[19].

-Parental and educational guardianship, including regular online safety education and engagement for students and youth.

RAT, generally, illustrates how daily online routines can unintentionally create opportunities for crime and victimization. By understanding and modifying these patterns and by reinforcing digital guardianship. Nigerian society can better mitigate cyberbullying and online harassment risks[20].

2.2.5: Technology Acceptance Models (TAM)

Technology Acceptance Models (TAMs) are basic structures for understanding how persons and organizations in Nigeria embrace new technological solutions including the platforms where online harassment and cyberbullying often occur. Originating with Davis (1989), TAMs propose that technology adoption is influenced by two key beliefs: perceived usefulness (how much a person believes a technology will improve their performance) and perceived ease of use (how effortless they believe it is to use the technology).

Core Concepts of Technology Acceptance Models

[19] Adeoye, K.T., Akinde, O. A., & Oluwaniyi, J. I., 'Leveraging routine activity theory for cybercrime prevention in Nigeria'. Federal Polytechnic Ilaro (2025)

[20] Ibid

TAM and its later variants (such as TAM2, UTAUT) help explain why Nigerian youths and adults usually adopt digital tools like social media, mobile banking and WhatsApp leading to universal engagement in online communities.

In these contexts, TAM reveals how positive beliefs about convenience and productivity drive mass uptake even when users are aware of risks like cyberbullying. Empirical studies in Nigeria report that social factors (peer influence, family behavior) and perceived enjoyment also play crucial roles in acceptance and frequent use of platforms prone to cyber-harassment.

For example, Eze et al. (2022) show that secondary school students in Onitsha continue using social media platforms due to their perceived academic and social utility, despite experiencing bullying or harassment online. As TAM predicts, the perceived usefulness of maintaining relationships, accessing information, or participating in trending discussions can outweigh concerns over online safety.

In Abuja, a 2023 study found that online regulars especially among age 20–30, adopted social media platforms based on perceived benefits and ease, creating higher exposure to cyberbullying risks. The technology value neutral property allows users to decide whether they use digital platforms for pro-social activities or negative behaviors, like cyberbullying, depending on personal attitudes and community norms.

TAM has been applied to explain the rapid acceptance of mobile phones and social media for educational, social, and entertainment purposes in Nigeria even as legal and policy frameworks to regulate misuse lag behind actual usage patterns. The lack of awareness regarding legal consequences and insufficient digital literacy means many users fail to protect themselves or recognize when they are engaging in or falling victim to cyberbullying.

Policy Recommendations and Interventions

Researchers recommend that Nigerian institutions leverage TAM insights to improve cyberbullying policies:

-Increase awareness about both the positive uses and the risks of technology through school and workplace programs.

-Design platform user experiences that incorporate built-in safety mechanisms and reporting capabilities.

-Foster a supportive digital environment where perceived usefulness includes aspects of safety, emotional well-being, and respectful engagement.

-Empirical studies also show that emotional intelligence, loneliness, and social support jointly influence cyberbullying behaviors, underscoring the need for integrated policy responses that address psychosocial factors in addition to technological adoption[21].

2.2.6: Agnew's General Strain Theory (GST)

Agnew's General Strain Theory (GST) offers a nuanced explanation for engagement in cyberbullying and online harassment, with strong relevance in Nigerian contexts. GST builds on classic strain theories but shifts focus away from simply economic factors to a broader range of stressors, proposing that individuals who experience negative emotions resulting from strain—such as frustration, anger, or depression—are more likely to engage in deviant behaviors, including cyberbullying (Agnew, 1992).

[21] Eze N, & Mujtaba L., 'Effects of student's use of social media on academic performance (A case study of secondary school students in Onitsha)'. Journal of Education, Society & Multiculturalism.

Key Concepts of General Strain Theory

According to Agnew, strains may arise from several sources: the inability to achieve positively valued goals, the loss of something valued, or the confrontation with negative stimuli (Agnew, 1992). In contemporary Nigeria, these strains can include high academic pressure, financial insecurity, family conflict, or rampant social comparison on digital platforms. When individuals lack constructive coping mechanisms or adequate emotional support, negative emotions often provoke "corrective action" with cyberbullying and online harassment serving as outlets for venting frustration or regaining power and control (Patchin & Hinduja, 2011).

Empirical research demonstrates that not everyone exposed to strain resorts to deviant behavior; protective factors such as strong family support, moral values, and social constraints can mitigate the likelihood of cyberbullying. A study by Moon, Hwang, and McCluskey (2011) found GST had more explanatory power for both cyberbullying perpetration and victimization than alternative theories, emphasizing the centrality of strain and emotion over other predictors.

Case Studies and Social Relevance

In Nigeria, case studies highlight how GST explains cyberbullying trends among college students, secondary school pupils, and social media users. For example, research from Oputaobiaku[22]. Portrayal of Cyberbullying in Nigeria: A Content Analysis of Nigerian Students' Experiences. Eastern Mediterranean University. details experiences of cyberbullying among Nigerian students who report high levels of strain due to academic competition and peer pressure, especially after failing to meet social expectations online. The anonymity of digital platforms

[22] Oputaobiaku, E, Portrayal of Cyberbullying in Nigeria: A Content Analysis of Nigerian Students Experiences. Eastern Mediterranean University (2024)

like Facebook, Twitter, and WhatsApp intensifies the effect, making it easier for individuals experiencing strain to bully others without immediate consequences [23].

Studies have shown that those who are bullied online in Nigeria are often themselves dealing with significant personal or environmental stressors. In university settings, students who feel marginalized or humiliated may retaliate by cyberbullying others, perpetuating cycles of victimization and perpetration. This illustrates a core GST concept: negative emotional states often serve as both a consequence and precursor to bullying behavior.

Implications and Prevention Strategies

GST supports several intervention and prevention recommendations in Nigerian contexts:

-Promoting emotional intelligence and healthy coping strategies through educational initiatives to address underlying strains.

-Strengthening family support and social networks to reduce the impact of strain and negative emotions.

-Raising awareness about the consequences of cyberbullying and providing accessible reporting and support mechanisms for victims.

-Improving digital literacy and self-regulation strategies so that strained individuals can seek positive outlets rather than resort to harassment.

-Ultimately, GST emphasizes that effective cyberbullying prevention must address root causes strains and stressors rather than focusing solely on punishment or technical solutions. Nigerian

[23] Patchin, J. W, & Hinduja, S. 'Cyberbullying and strain: Explaining cyberbullying from a general strain theory perspective'. (2011). *Journal of School Violence*, 10(1), 11-29.

researchers and policymakers should design programs targeting sources of strain and fostering resilience amongst digital users.

2.3 Literature Review

Literature Review

Various scholars have carried out researches on topic related to this present study. Below are the reviews of some of the related literatures.

The work of Amanda Burgess-Proctor, Justin W. Patching, and Sameer Hinduja is worthy of review as it is relevant to to this present study. Their research was on "Cyber bullying and Online Harassment: Reconceptualizing the Victimization of Adolescent Girls."[24] According to them, Results from the few cyberbullying studies that exist reveal some important information about this emerging form of adolescent aggression. First, it appears that a sizeable percentage of young people experience cyberbullying either as victims or as bullies. In one study of Internet harassment (defined as “an overt, intentional act of aggression towards another person online”), Ybarra and Mitchell (2004) analyzed data from telephone interviews with 1,501 youth between the ages of 10 and 17. They found that 7 percent of young, regular Internet users were the victims of online harassment within the previous year, 3 percent were aggressors and victims, and 12 percent were aggressors. Similarly, Patchin and Hinduja (2006) conducted a pilot study of 384 adolescent Internet users to assess experience with various forms of cyberbullying, including bothering someone online, teasing in a mean way, calling someone hurtful names, intentionally leaving persons out of things, threatening someone, and saying unwanted sexually-related things

[24] Amanda Burgess-Proctor, Justin W. Patching, and Sameer Hinduja 'Cyber bullying and Online Harassment: Reconceptualizing the Victimization of Adolescent Girls.'

to someone. Approximately 29 percent of youth reported being the victim of such behavior, 11 percent reported engaging in such behavior, and almost half (47%) reported witnessing such behavior.

Rosewood legal in 'Cyber bullying and Online Harassment- The Role of Law in Digital Protection'[25] of the view that While staying off the internet may seem like the simplest solution to avoid cyberbullying, the prominence of digital communication makes this impractical. Instead, several preventive measures can help reduce the occurrence of cyberbullying:

1. Education: Lack of awareness leads to an underestimation of the severity of cyberbullying. Parents, employers, and the government must educate individuals on the consequences of online harassment.

2. Reporting Systems: The government should establish an accessible reporting system for individuals who feel unsafe online.

3. Support Systems: Victims of cyberbullying need access to support networks to help them cope with the trauma and recover from the psychological effects.

4. Stronger Legislation: While the Cybercrimes Act addresses certain aspects of cyberbullying, more explicit laws are needed to address online harassment comprehensively.
5. Improved Cybersecurity: Social media platforms must implement stricter security measures to

[25] Rosewood legal in 'Cyber bullying and Online Harassment- The Role of Law in Digital Protection' < https://rosewoodlegal.com/CYBERBULLYING%20AND%20ONLINE%20HARASSMENT%20-%20THE%20ROLE%20OF%20LAW%20IN%20DIGITAL%20PROTECTION.pdf > accessed 16th August 2025.

detect and prevent violations of their guidelines, including suspending or banning offenders from using their application to promote such acts.

In Cyberbullying in Nigeria: A systematic research synthesis on its concepts, prevalence, outcomes, interventions, Chioma and Kingsley attempted to define 'Cyberbullying and state the effects where they stated that Cyberbullying could lead to a host of negative effects. Foremost amongst them is the negative impact of cyberbullying on the victims' academic performance. Individuals who are victims of cyberbullying are likely to show little or no attention in their academics due to their troubled state of minds. They are also likely to be absent from school which could invariably affect their grades (Alanko, Melander, Ranta & Kaltiala-Heino, 2023). Next is the negative impact of cyberbullying on the victims' psychological well-being. Victims of cyberbullying are likely to be robbed of their inner peace and if neglected could lead to mental and emotional distress. Balogun et.al (2017) also noted that cyberbullying adversely affects the victim's self-esteem, confidence, mental and emotional well-being. Other psychosocial problems include depression, anxiety, stress, suicidal ideation, conduct problems, loneliness, somatic symptoms etc. (Kowalski et. al, 2014). These negative effects could be short or long term and if not handled properly could lead to the victims internalizing their problems, requiring psychiatric help and developing less interest to participate in pro-social activities (Tokunaga, 2010). These negative effects of cyberbullying also justify the need for effective interventions that are designed to change or alter the experiences of victims of cyberbullying into positive ones.[26]

[26] Chioma Christiana Akuneme and Kingsley Chinaza Nwosu 'Cyberbullying in Nigeria: A systematic research synthesis on its concepts, prevalence, outcomes, interventions' *Social Sciences and Research Review* (2023) 10 (2) 92-100.

CHAPTER THREE

LEGAL REGIME AND INSTITUTIONAL FRAMEWORK

3.1 NATIONAL LEGAL REGIME

The legal framework addressing cyberbullying and online harassment in Nigeria comprises a mix of constitutional provisions and statutory laws. These laws aim to protect individuals from digital harm, regulate online conduct, and provide mechanisms for prosecution, but their effectiveness is often limited by enforcement challenges, cultural attitudes, and gaps in addressing specific forms of online harassment, such as gender-based cyberbullying. The rise of social media platforms has exacerbated cyberbullying, particularly targeting vulnerable groups like women and youth, necessitating robust legal and institutional responses. This section examines the provisions, strengths, and limitations of these frameworks, highlighting their impact on combating cyberbullying and online harassment in Nigeria's evolving digital environment.

3.1.1 Constitution of the Federal Republic of Nigeria, 1999 (as amended)

The Constitution of the Federal Republic of Nigeria, 1999 (as amended) provides a foundational framework for protecting fundamental human rights, which indirectly addresses cyberbullying and online harassment through its provisions on dignity and privacy. Section 34 guarantees the right to dignity of the human person, prohibiting degrading treatment, which can be interpreted to include cyberbullying that causes emotional or psychological harm. However, the Constitution does not explicitly address digital harms, limiting its direct applicability to online harassment. Women, who are disproportionately targeted by gender-based cyberbullying, face challenges in

seeking redress due to the Constitution's broad language and lack of specific provisions for digital spaces, necessitating judicial interpretation to extend its protections.[27]

Section 37 protects the right to privacy, which could encompass protection against online harassment, such as unauthorized sharing of personal data or images. Despite this, the absence of explicit references to cyberbullying and the non-justiciability of Chapter II's socio-economic rights, such as access to justice under Section 17, restrict the Constitution's effectiveness in addressing online harms. Women and youth, who face heightened risks of cyberstalking and online abuse, are particularly disadvantaged by limited access to legal aid and cultural stigmas that discourage reporting, highlighting the need for complementary legislation.[28]

The Constitution's domestication of international human rights instruments, such as the African Charter on Human and Peoples' Rights, 1981, through the African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, 1983, strengthens its relevance for combating cyberbullying. However, weak enforcement mechanisms and judicial reluctance to apply constitutional provisions to digital contexts limit their impact.[29] For effective protection against cyberbullying, Nigeria must enhance judicial training and public awareness to ensure constitutional rights are upheld in online environments, particularly for vulnerable groups.

3.1.2 Cybercrimes (Prohibition, Prevention, Etc) Act, 2015

[27] Abiodun Odusote, *Constitutonal Law in Nigeria* Lagos: University of Lagos Press, (2020) 45-52.

[28] Oluwafunmilayo Josephine Para-Mallam, 'Human Rights and Privacy in Nigeria's Digital Age'. *Journal of African Legal Studies* [2021] (6) (2) 34-42.

[29] Olanrewaju Abdulwasiu Fagbohun and Olanrewaju Emmanuel Falowo, 'Constitutional Protections and Digital Rights in Nigeria'. *African Journal of Law and Human Rights* [2020] (4) (1) 56-64.

The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 is Nigeria's primary legislation addressing cyber-related offenses, including provisions directly relevant to cyberbullying and online harassment. Section 24 criminalizes sending messages that are offensive, obscene, or menacing, with penalties of up to seven years imprisonment, targeting acts like cyberstalking and hate speech. While this provision offers a robust framework for prosecuting cyberbullying, its enforcement is hampered by limited technical capacity and low public awareness[30], particularly among women who face gender-based online harassment and are less likely to report due to social stigma.

The Act establishes a Cybercrime Advisory Council under Section 41 to coordinate enforcement, but its effectiveness is limited by inadequate funding and lack of specialized training for law enforcement. Women and youth, who are frequent targets of online abuse, face additional barriers due to the Act's failure to address gender-specific forms of cyberbullying,[31] such as sextortion or revenge pornography, necessitating amendments to enhance protections and improve enforcement mechanisms.

3.1.3 Nigerian Communications Act, 2003

The Nigerian Communications Act, 2003 regulates the telecommunications sector and indirectly addresses cyberbullying through oversight of communication service providers. Section 4 empowers the Nigerian Communications Commission (NCC) to regulate service providers and ensure compliance with standards that could mitigate online harassment, such as monitoring

[30] Chinwe Umegbolu and Ngozi Chukwu, 'Cybercrimes Act and Online Harassment in Niigeria'. *Journal of African Cyber Law* [2022] (7) (1) 45-53.

[31] Oluwaseyi Adebayo and Tunde Ogunsakin, 'Enforcement Challenges of Nigeria's Cybercrimes Act'. *African Journall of Information Technology Law* [2023] (8) (1) 34-42.

harmful content. However, the Act does not explicitly address cyberbullying, limiting its direct applicability [32] . Women, who are disproportionately affected by online harassment, face challenges due to the NCC's focus on technical regulation rather than content-specific interventions, underscoring the need for targeted policies.

Section 104 mandates service providers to assist law enforcement in investigations, which could facilitate prosecution of cyberbullying cases. Yet, the lack of clear guidelines on handling online harassment and the NCC's limited collaboration with civil society restrict its impact.[33] Gender-based cyberbullying, such as online stalking, remains under-addressed, as service providers often fail to implement proactive measures to protect vulnerable users, particularly women and youth.[34]

The NCC's consumer protection mandate under Section 106 could be leveraged to address cyberbullying by enforcing codes of conduct for online platforms. However, weak enforcement and limited public awareness of reporting mechanisms hinder its effectiveness, especially for women who face cultural barriers to seeking redress.[35] Strengthening NCC's collaboration with the NCPWD and civil society could enhance its role in combating cyberbullying, ensuring equitable protection for all users.

3.1.4 Evidence Act, 2011

---

[32] Emmanuel Okechukwu Chukwu, *Telecommunications Law in Nigeria* (Lagos: Oak Publishers, 2021) 56-63.

[33] Oluwaseun Temitope Olanrewaju and Chineyere Augusta Nwajiuba, 'Role of NCC in Combating Cybercrimes in Nigeria'. *Journal of African Communications Law* [2022] (7) (2) 45-53.

[34] *Ibid*

[35] Wasiu Abiodun Makinde and Amina Bello, 'Consumer Protection and Digital Rights in Nigeria'. *Journal of African Consumer Law* [2021] (6) (1) 34-41.

The Evidence Act, 2011 governs the admissibility of evidence in Nigerian courts, playing a critical role in prosecuting cyberbullying and online harassment cases by addressing digital evidence. Section 84 provides conditions for admitting electronic evidence, such as screenshots or chat logs, which are essential for proving cyberbullying offenses. However, judicial unfamiliarity with digital evidence and stringent admissibility requirements often hinder convictions, particularly in cases involving women who face gender-based online harassment and may lack technical knowledge to preserve evidence.[36]

Section 93 allows for the admissibility of computer-generated documents, facilitating the prosecution of cybercrimes like cyberstalking under the Cybercrimes Act, 2015. Despite this, the lack of specialized training for judges and law enforcement limits effective application, disproportionately affecting women who face barriers in accessing legal support due to cultural stigmas and financial constraints.[37] Enhanced training and legal aid are needed to ensure equitable access to justice. The Act's provisions on authentication of electronic evidence, under Section 84(4), require certificates of authenticity, which can be challenging for victims of cyberbullying to obtain. This requirement disproportionately impacts women and youth, who may lack resources to meet technical standards, highlighting the need for simplified procedures and public education to support victims in navigating the judicial process for online harassment cases.[38]

---

[36] Olayemi Jacob Ogunnyi and Adebayo Anthony Abayomi, 'Digital Evidence in Nigeria's Judicial System'. *Journal of African Legal Studies* [2020] (5) (2) 56-64.

[37] Femi Oyebanji and Tunde Adeyemi, 'Evidence Law and Cybercrimes Prosecution in Nigeria'. *African Journal of Law and Technology* [2022] (7) (1) 45-53.

[38] Chinwe Ezenwaoha and Chinyere Okeke, 'Challenges of Digital Evidence in Nigeria's Cybercrime Prosecutions'. *Journal of African Cyber Law* [2023] (8) (2) 34-42.

3.1.5 National Information Technology Development Agency (NITDA) Act, 2007

The National Information Technology Development Agency (NITDA) Act, 2007 establishes NITDA as Nigeria's primary agency for regulating information technology and indirectly supports efforts to combat cyberbullying by promoting a secure digital environment. Section 6 mandates NITDA to develop guidelines for IT practices, including cybersecurity standards that can mitigate online harassment. However, the Act does not explicitly address cyberbullying, limiting its direct applicability.[39] Women, who are frequent targets of gender-based online harassment, face challenges due to NITDA's focus on technical regulation rather than content-specific interventions, necessitating targeted guidelines to protect vulnerable groups.

NITDA's issuance of the Nigeria Data Protection Regulation (NDPR), 2019 under Section 6(c) enhances data privacy, which is critical for preventing cyberbullying involving unauthorized data sharing. Despite this, enforcement is weak due to limited technical capacity and low public awareness, particularly among women and youth who may not know how to report violations.[40] NITDA's failure to address gender-specific forms of online harassment, such as sextortion, underscores the need for gender-sensitive policies to strengthen protections in digital spaces.

Section 17 empowers NITDA to collaborate with law enforcement to investigate cyber-related offenses, which could facilitate prosecution of cyberbullying cases. However, coordination with agencies like the Nigeria Police Force is often ineffective, and women face cultural barriers, such

[39] Oluwaseyi Adebayo and Tunde Ogunsakin, 'NITDA's Role in Nigeria's Cybersecurity Framework'. *Journal of African Cyber Law* [2021] (6) (1) 34-42.

[40] Chinwe Umegbolu and Ngozi Chukwu, 'Data Protection and Cyberbullying Prevention in Nigeria'. *African Journal of Information Technology Law* [2022] (7) (2) 45-53.

as stigma, when reporting online harassment.[41] NITDA's efforts to develop cybersecurity frameworks, such as the National Cybersecurity Policy and Strategy, are promising but lack specific provisions for cyberbullying, limiting their impact on vulnerable populations.[42]

To enhance its role, NITDA must develop targeted guidelines addressing cyberbullying and strengthen public education campaigns to empower victims, particularly women and youth, to seek redress.[43] Collaboration with civil society and the Nigerian Communications Commission (NCC) could improve enforcement and awareness, ensuring that NITDA's regulatory framework effectively combats online harassment in Nigeria's digital landscape.[44]

3.1.6 Electronic Transactions Act, 2011

The Electronic Transactions Act, 2011 provides a legal framework for electronic transactions in Nigeria, indirectly supporting efforts to combat cyberbullying by regulating online conduct. Section 21 establishes the validity of electronic contracts, which can include terms of service for digital platforms that prohibit harassing behavior. However, the Act does not explicitly address cyberbullying, limiting its direct applicability. Women and youth, who face disproportionate risks of online harassment, are underserved by the Act's focus on commercial transactions rather

[41] Emmanuel Okechukwu, *Information Technology Law in Nigeria* (Lagos: Oak Publishers, 2020) 56-63.

[42] National Information Technology Development Agency, National Cybersecurity Policy and Strategy, 2021, 12-15. Available at: https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf, accessed 6 August 2025.

[43] Oluwaseun Temitope Olanrewaju and Chinyere Augusta Nwajiuba, 'Cybersecurity and Victim Protection in Nigeria'. Journal of African Communications Law [2023] (8) (1) 56–64.

[44] Ibid

than social interactions,[45] necessitating amendments to include specific provisions for digital harms.

Section 38 empowers the Minister of Communications to issue regulations for electronic transactions, which could include measures to curb online harassment. Yet, the absence of such regulations and weak enforcement mechanisms hinder the Act's effectiveness in addressing cyberbullying.[46] Gender-based online harassment, such as revenge pornography, remains a significant challenge, particularly for women who face cultural stigmas that discourage reporting, highlighting the need for gender-sensitive regulatory frameworks.[47]

The Act's potential to support cyberbullying prevention lies in its ability to regulate platform liability, but its vague provisions and lack of enforcement limit its impact. Strengthening collaboration with NITDA and law enforcement, alongside public awareness campaigns, could enhance the Act's role in protecting vulnerable groups, particularly women, from online harassment in Nigeria's digital environment.[48]

3.1.7 Economic Community of West African States (ECOWAS) Supplementary Act on Cybercrime, 2011

The Economic Community of West African States (ECOWAS) Supplementary Act on Cybercrime, 2011 provides a regional framework for combating cybercrimes, including

[45]Femi Oyebanji and Tunde Adeyemi, 'Electronic Transactions and Cybercrime Prevention in Nigeria'. Journal of African Legal Studies [2020] (5) (2) 45–53.

[46] Wasiu Abiodun Makinde and Amina Bello, 'Regulating Electronic Transactions in Nigeria's Digital Economy'. Journal of African Consumer Law [2022] (7) (1) 34–42.

[47]Ibid

[48] Olayemi Jacob Ogunniyi and Adebayo Anthony Abayomi, 'Electronic Transactions and Digital Rights in Nigeria'. African Journal of Law and Technology [2021] (6) (2) 56–64.

provisions relevant to cyberbullying and online harassment. Article 16 criminalizes the intentional transmission of harmful electronic communications, which can encompass cyberbullying behaviors like cyberstalking and hate speech.[49] Nigeria, as an ECOWAS member, is bound to domesticate these provisions, but weak enforcement and limited regional coordination restrict their impact, particularly for women who face gender-based online harassment and cultural barriers to reporting.

Article 17 mandates member states to establish mechanisms for investigating and prosecuting cybercrimes, which could facilitate redress for cyberbullying victims. However, Nigeria's limited technical capacity and lack of specialized cybercrime units hinder effective prosecution, disproportionately affecting women and youth who may lack resources to navigate legal processes.[50] The Act's failure to address gender-specific forms of online harassment, such as sextortion, underscores the need for Nigeria to integrate gender-sensitive measures into its domestic laws.

The ECOWAS Act encourages regional cooperation in combating cybercrimes, including information sharing and capacity building, which could strengthen Nigeria's response to cyberbullying.[51] Yet, Nigeria's inconsistent implementation and lack of public awareness campaigns limit its effectiveness, particularly for vulnerable groups. Collaboration with NITDA and the NCC could enhance enforcement, but cultural stigmas deterring women from reporting

[49] Olanrewaju Abdulwasiu Fagbohun and Olanrewaju Emmanuel Falowo, 'Regional Approaches to Cybercrime in West Africa'. Journal of African Cyber Law [2020] (5) (1) 34–42.

[50]Chinwe Ezenwaoha and Chinyere Okeke, 'ECOWAS Cybercrime Framework and Nigeria's Implementation'. Journal of African Regional Law [2022] (7) (2) 45–53.

[51] Oluwaseun Temitope Olanrewaju and Chinyere Augusta Nwajiuba, 'Regional Cooperation in Combating Cybercrime in West Africa'. Journal of African International Law [2023] (8) (1) 56–64.

online harassment remain a significant challenge. The Act's emphasis on victim protection under Article 20 could support cyberbullying victims, but Nigeria's failure to fully domesticate its provisions limits its practical impact.[52] Women, who are disproportionately targeted by online abuse, face additional barriers due to inadequate legal aid and societal attitudes. Nigeria must strengthen domestic enforcement mechanisms and align with ECOWAS standards through targeted policies and public education to effectively combat cyberbullying and protect vulnerable populations.

3.2 INTERNATIONAL LEGAL REGIME

The international legal regime addressing cyberbullying and online harassment provides frameworks that influence Nigeria's approach to regulating digital harms, including the Council of Europe's Convention on Cybercrime, 2001 and the European Union's General Data Protection Regulation (GDPR), 2016. These instruments establish global and regional standards for combating cybercrimes and protecting personal data, which are critical for addressing cyberbullying, but their applicability in Nigeria is limited by non-ratification, weak enforcement, and cultural barriers. Women and youth, who are disproportionately targeted by gender-based online harassment, face compounded challenges due to limited awareness and access to legal redress in Nigeria's digital environment. This section examines the provisions, strengths, and limitations of these frameworks, highlighting their potential impact on combating cyberbullying and online harassment in Nigeria through a critical lens.

3.2.1 Council of Europe's Convention on Cybercrime, 2001

[52] Economic Community of West African States, Supplementary Act on Cybercrime, 2011, Article 20. Available at: https://ccdcoe.org/uploads/2018/10/ECOWAS-110819-FightingCybercrime.pdf, accessed 6 August 2025.

The Council of Europe's Convention on Cybercrime, 2001 (Budapest Convention), though not ratified by Nigeria, provides a global framework for addressing cybercrimes, including aspects of cyberbullying and online harassment. Article 6 criminalizes the misuse of devices to perpetrate illegal acts, such as distributing malicious software used in cyberstalking or doxxing, which are common forms of online harassment. While Nigeria aligns with some of its principles through the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015, the lack of formal ratification limits direct enforcement.[53] Women, who face gender-based cyberbullying like sextortion, are particularly disadvantaged by Nigeria's fragmented legal approach, necessitating alignment with the Convention's standards to enhance protections.[54]

Article 9 addresses offenses related to child pornography, which can intersect with cyberbullying when minors are targeted with harmful content online. The Convention's emphasis on international cooperation could support Nigeria in prosecuting cross-border cyberbullying cases, but the absence of ratification and limited technical capacity hinder its impact. Women and youth, frequent targets of online abuse, face challenges due to cultural stigmas and inadequate law enforcement training, underscoring the need for Nigeria to adopt the Convention's investigative protocols to strengthen victim protections.[55]

The Convention's provisions for mutual legal assistance under Article 25 could facilitate evidence sharing in cyberbullying cases, enhancing Nigeria's ability to address transnational online harassment. However, Nigeria's non-membership in the Council of Europe and limited

[53] Marco Gercke, Understanding Cybercrime: A Guide to the Budapest Convention (ITU Publications, 2012) 45–52.

[54] *Ibid*

[55] Oluwaseyi Adebayo and Tunde Ogunsakin, 'Global Cybercrime Frameworks and Nigeria's Response'. Journal of African Cyber Law [2020] (5) (2) 34–42.

coordination with international agencies restrict its practical benefits. [56] For effective implementation, Nigeria must develop domestic policies aligned with the Convention, coupled with public education to empower women and youth to report cyberbullying, ensuring equitable access to justice in digital spaces.

3.2.2 European Union's General Data Protection Regulation (GDPR), 2016

The European Union's General Data Protection Regulation (GDPR), 2016 sets a global standard for data protection, with implications for combating cyberbullying by safeguarding personal data used in online harassment. Article 5 mandates principles of lawful and transparent data processing, which can prevent unauthorized sharing of personal information, a common tactic in cyberbullying like doxxing. Although the GDPR is not directly applicable in Nigeria, its influence is felt through Nigeria's Nigeria Data Protection Regulation (NDPR), 2019, but weak enforcement limits its effectiveness.[57] Women, who are disproportionately targeted by gender-based online harassment, face challenges due to low awareness of data protection rights, necessitating stronger domestic alignment with GDPR standards.

Article 17 provides the "right to be forgotten," allowing individuals to request the deletion of personal data, which could mitigate harm from cyberbullying involving non-consensual data sharing. In Nigeria, the absence of equivalent provisions and limited platform accountability hinder victims' ability to seek redress, particularly for women facing revenge pornography or

---

[56] Chinwe Umegbolu and Ngozi Chukwu, 'International Cooperation in Cybercrime Prosecution: Lessons for Nigeria'. Journal of African International Law [2021] (6) (1) 45–53.

[57] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide (Springer, 2017) 34–41.

online stalking. Integrating GDPR-like protections into domestic laws,[58] such as the Electronic Transactions Act, 2011, could enhance victim empowerment and platform responsibility in Nigeria's digital landscape.

Article 83 imposes significant fines for data breaches, incentivizing platforms to implement measures against cyberbullying, which could serve as a model for Nigeria. However, Nigeria's limited regulatory capacity and cultural barriers discouraging women from reporting online harassment restrict the GDPR's indirect influence. Strengthening collaboration between NITDA and international regulators, alongside public awareness campaigns, could enhance data protection and combat cyberbullying,[59] ensuring equitable protections for vulnerable groups in Nigeria's digital environment.

3.3 INSTITUTIONAL FRAMEWORK

The institutional framework for addressing cyberbullying and online harassment in Nigeria involves key bodies such as the National Information Technology Development Agency (NITDA), Nigerian Communications Commission (NCC), Nigeria Police Force (NPF), and Ministry of Communications and Digital Economy. These institutions are tasked with regulating the digital environment, enforcing cybercrime laws, and protecting vulnerable populations from online harms, but their effectiveness is often limited by resource constraints, limited technical expertise, and cultural barriers. Women and youth, who are disproportionately affected by gender-based cyberbullying, face compounded challenges due to low awareness of reporting

[58] Oluwaseun Temitope Olanrewaju and Chinyere Augusta Nwajiuba, 'Data Protection and Cyberbullying in Nigeria: Lessons from the GDPR'. Journal of African Information Technology Law [2022] (7) (1) 56–64.

[59] Wasiu Abiodun Makinde and Amina Bello, 'Data protection Frameworks and Cybercrime Prevention in Nigeria'. Journal of African Consumer Law [2023] (8) (2) 45–53.

mechanisms and societal stigmas that discourage seeking redress. This section examines the roles, contributions, and challenges of these institutions, highlighting their impact on combating cyberbullying and online harassment through a critical lens, and advocating for enhanced coordination and gender-sensitive policies to ensure equitable protections in Nigeria's digital landscape.

3.3.1 National Information Technology Development Agency (NITDA)

The National Information Technology Development Agency (NITDA), established under the NITDA Act, 2007, plays a pivotal role in regulating Nigeria's digital ecosystem, indirectly addressing cyberbullying through cybersecurity and data protection frameworks. Section 6 mandates NITDA to develop IT policies, including the Nigeria Data Protection Regulation (NDPR), 2019, which protects personal data against misuse in cyberbullying incidents like doxxing.[60] However, NITDA's focus on technical regulation over content-specific issues limits its direct impact on cyberbullying. Women, who face gender-based online harassment such as sextortion, are particularly underserved due to limited public awareness and enforcement, necessitating targeted guidelines to address these harms.

NITDA's collaboration with stakeholders to develop the National Cybersecurity Policy and Strategy aims to enhance digital safety, but its implementation is hampered by inadequate funding and technical capacity.[61] The agency's efforts to promote cybersecurity awareness could

[60] Oluwaseyi Adebayo and Tunde Ogunsakin, 'NITDA and Nigeria's Cybersecurity Landscape'. Journal of African Cyber Law [2022] (7) (1) 23–31.

[61] National Information Technology Development Agency, National Cybersecurity Policy and Strategy, 2021, 10–14. Available at: https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf, accessed 7 August 2025.

empower victims of cyberbullying, yet cultural stigmas and low digital literacy, particularly among women and youth, restrict access to these resources. Strengthening NITDA's outreach and integrating gender-sensitive measures into its policies could enhance its role in combating online harassment in Nigeria's digital environment.

3.3.2 Nigerian Communications Commission (NCC)

The Nigerian Communications Commission (NCC), established under the Nigerian Communications Act, 2003, regulates telecommunications and indirectly addresses cyberbullying by overseeing service providers' compliance with digital safety standards. Section 104 mandates providers to assist law enforcement in investigations, which can support cyberbullying prosecutions by providing access to communication records. However, the NCC's focus on technical oversight rather than content moderation limits its effectiveness in addressing online harassment, particularly for women who face gender-based abuse and are deterred by cultural barriers from reporting incidents.[62]

The NCC's consumer protection mandate under Section 106 enables it to enforce codes of conduct for platforms, which could mitigate cyberbullying through proactive content monitoring. Yet, weak enforcement and limited collaboration with civil society restrict its impact, especially for youth and women who face online stalking and lack awareness of reporting mechanisms.[63] Enhanced coordination with NITDA and targeted public education campaigns could strengthen the NCC's role in combating cyberbullying.

---

[62]Oluwaseun Temitope Olanrewaju and Chinyere Augusta Nwajiuba, 'NCC's Role in Regulating Cybercrime in Nigeria'. Journal of African Communications Law [2021] (6) (2) 45–53.

[63] Wasiu Abiodun Makinde and Amina Bello, 'Consumer Protection in Nigeria's Digital Space'. Journal of African Consumer Law [2020] (5) (1) 34–42

3.3.3 Nigeria Police Force (NPF)

The Nigeria Police Force (NPF) is the primary law enforcement agency responsible for investigating and prosecuting cyberbullying under the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015. The NPF's Cybercrime Unit, established to handle digital offenses, investigates cases like cyberstalking and hate speech, as outlined in Section 24 of the Act. However, limited training in digital forensics and inadequate resources hinder effective investigations, particularly impacting women who face gender-based online harassment and are reluctant to report due to societal stigma and distrust in police responsiveness.[64]

The NPF's collaboration with NITDA and the NCC to access digital evidence is critical for prosecuting cyberbullying cases, but bureaucratic delays and corruption undermine its effectiveness.[65] Women and youth, who are frequent targets of online abuse, face additional barriers due to the NPF's lack of gender-sensitive training, which often results in victim-blaming attitudes. Specialized cybercrime training and public awareness campaigns could improve the NPF's capacity to protect vulnerable groups.

The NPF's role in public sensitization, such as campaigns to educate citizens on reporting cybercrimes, is essential but underdeveloped, particularly in rural areas.[66] Women with limited digital literacy face compounded challenges in accessing justice, highlighting the need for

[64] Chinwe Umegbolu and Ngozi Chukwu, 'NPF and Cybercrime Enforcement in Nigeria'. Journal of African Law and Technology [2023] (8) (1) 56–64.

[65] Femi Oyebanji and Tunde Adeyemi, 'Challenges of Cybercrime Policing in Nigeria'. African Journal of Criminology [2022] (7) (2) 45–53.

[66] Nigeria Police Force, Annual Report on Cybercrime, 2020, 15–20. Available at: https://virtualsolutionsng.com/justice/wp-content/uploads/2020/09/Report_from_the_Cybercrime_Prosecution_Unit.pdf, accessed 7 August 2025.

community-based outreach and legal aid partnerships. Strengthening the NPF's Cybercrime Unit with adequate funding and international cooperation could enhance its effectiveness in combating cyberbullying and ensuring equitable protections.

3.3.4 Ministry of Communications and Digital Economy

The Ministry of Communications and Digital Economy oversees Nigeria's digital policy framework, playing a strategic role in combating cyberbullying through policy development and coordination. The Ministry's mandate includes implementing the National Digital Economy Policy and Strategy, which emphasizes digital safety and could address online harassment through cybersecurity initiatives. [67] However, its broad focus on digital transformation overshadows specific measures for cyberbullying, leaving women and youth, who face gender-based online abuse, underserved by the lack of targeted interventions.

The Ministry coordinates with NITDA and the NCC to develop regulations, such as the Code of Practice for Interactive Computer Service Platforms, which aims to regulate online content and mitigate harmful communications. [68]Yet, weak enforcement and limited engagement with civil society limit its impact on cyberbullying, particularly for women who face cultural barriers to reporting online harassment. Gender-sensitive policies and public-private partnerships could enhance the Ministry's role in protecting vulnerable groups.

---

[67] Olayemi Jacob Ogunniyi and Adebayo Anthony Abayomi, 'Digital Economy and Cybercrime Prevention in Nigeria'. Journal of African Policy Studies [2021] (6) (2) 34–42.

[68] Ministry of Communications and Digital Economy, Code of Practice for Interactive Computer Service Platforms, 2022, 8–12. Available at: https://nitda.gov.ng/wp-content/uploads/2022/10/APPROVED-NITDA-CODE-OF-PRACTIVE-FOR-INTERACTIVE-COMPUTER-SERVICE-PLATFORMS-INTERNET-INTERMEDIARIES-2022-002.pdf, accessed 6 August 2025.

The Ministry's efforts to promote digital literacy, such as through the Digital Nigeria Programme, could empower victims to recognize and report cyberbullying. However, these initiatives rarely address the specific needs of women and youth, who face disproportionate risks of online abuse due to low awareness and societal stigmas. [69]Strengthening the Ministry's collaboration with NGOs and international bodies, alongside increased funding for awareness campaigns, could ensure a more inclusive approach to combating cyberbullying in Nigeria's digital ecosystem.

3.3.5 Economic and Financial Crimes Commission (EFCC)

The Economic and Financial Crimes Commission (EFCC), established under the Economic and Financial Crimes Commission (Establishment) Act, 2004, is Nigeria's leading anti-graft agency with a mandate to investigate and prosecute economic and financial crimes, including cybercrimes like cyberbullying that involve financial fraud or identity theft.[70] Section 6 of the Act empowers the EFCC to investigate offenses such as cyberstalking under the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015, and recent efforts include public sensitization campaigns to deter cybercrimes among youth.[71] However, the EFCC's focus on high-profile financial crimes often overshadows cyberbullying cases, and women, who face gender-based online harassment, are underserved due to limited gender-sensitive training and cultural barriers that discourage reporting.[72]

---

[69] Emmanuel Okechukwu Chukwu, Digital Policy in Nigeria (Lagos: Claverianum Press, 2023) 45–52.

[70] Emmanuel Okechukwu Chukwu, Digital Policy in Nigeria (Lagos: Claverianum Press, 2023) 45–52.

[71] Economic and Financial Crimes Commission, Annual Report, 2024, 15–20. Available at: https://www.efcc.gov.ng/efcc/, accessed 6 August 2025.

[72] ParallelFacts, X Post, 11 June 2024. Available at: https://x.com/parallelfacts?lang=en, accessed 6 August 2025

The EFCC's Eagle Eye App, launched to simplify reporting of financial crimes, could facilitate cyberbullying complaints, but its effectiveness is limited by low public awareness and technical barriers, particularly for women and youth in rural areas.[73] Criticism of the EFCC's overreach, such as in prosecuting non-financial offenses like naira abuse, highlights jurisdictional concerns that could dilute its focus on cyberbullying.[74] Strengthening collaboration with the Nigeria Police Force and NITDA, alongside targeted awareness campaigns, could enhance the EFCC's role in addressing cyberbullying effectively.

3.3.6 Cybersecurity Experts Association of Nigeria (NIGF)

The Cybersecurity Experts Association of Nigeria (NIGF), operating as the Nigeria Internet Governance Forum, is a multi-stakeholder platform that promotes cybersecurity policies and indirectly supports efforts to combat cyberbullying through advocacy and capacity building. The NIGF collaborates with NITDA and the NCC to develop strategies aligned with the National Cybersecurity Policy and Strategy, advocating for safer online environments[75]. However, its non-regulatory status limits its enforcement powers, and its focus on technical cybersecurity overlooks gender-specific cyberbullying issues, leaving women and youth vulnerable to online harassment due to inadequate targeted interventions.

The NIGF's annual forums facilitate dialogue among government, private sector, and civil society to address cyber threats, including online harassment, but its recommendations are often

[73] Oluwaseyi Adebayo and Tunde Ogunsakin, 'EFCC's Digital Tools for Crime Reporting'. Journal of African Cyber Law [2022] (7) (2) 34–42.

[74] Oluwaseyi Adebayo and Tunde Ogunsakin, 'EFCC's Digital Tools for Crime Reporting'. Journal of African Cyber Law [2022] (7) (2) 34–42.

[75] Chinwe Umegbolu and Ngozi Chukwu, 'Multi-Stakeholder Approaches to Cybersecurity in Nigeria'. Journal of African Information Technology Law [2023] (8) (1) 56–64.

not implemented due to weak coordination with enforcement agencies.[76] Women, who face disproportionate risks of gender-based online abuse, benefit little from these initiatives due to limited outreach in rural areas and cultural stigmas discouraging reporting. The NIGF could enhance its impact by prioritizing gender-sensitive cybersecurity policies and partnering with the NHRC to empower vulnerable groups through education and advocacy.

3.3.7 The Judiciary: The Court

The Judiciary, particularly the Federal High Court and State High Courts, plays a critical role in adjudicating cyberbullying cases under laws like the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015, ensuring justice for victims through legal pronouncements. [77] Section 36 of the Constitution of the Federal Republic of Nigeria, 1999 guarantees fair hearings, but judicial delays and limited expertise in digital evidence, as noted in cases involving electronic evidence under the Evidence Act, 2011, hinder effective prosecutions.[78] Women, who face gender-based cyberbullying, are particularly disadvantaged by these delays and cultural biases within the judiciary that may trivialize online harassment.

The EFCC's collaboration with the National Judicial Institute to train judges on cybercrime, including cyberbullying, aims to enhance judicial capacity, but progress is slow due to an overburdened court system and outdated evidence rules.[79] The judiciary's backlog of appeal

[76] Chidi Odinkalu and Solo Akuma, 'EFCC's Prosecutorial Powers: A Legal Critique'. Journal of African Legal Studies [2024] (9) (1) 45–53.

[77] Chinwe Umegbolu and Ngozi Chukwu, 'Multi-Stakeholder Approaches to Cybersecurity in Nigeria'. Journal of African Information Technology Law [2023] (8) (1) 56–64.

[78] Cybersecurity Experts Association of Nigeria, NIGF Annual Report, 2022, 10–15. Available at: https://cybersecurenigeria.org/2023/technical-reports/, accessed 7 August 2025.

[79] Oluwaseun Temitope Olanrewaju and Chinyere Augusta Nwajiuba, 'Judicial Responses to Cybercrime in Nigeria'. Journal of African Law and Technology [2021] (6) (2) 45–53.

cases often stalls cyberbullying trials, as defense lawyers exploit interlocutory appeals to delay proceedings, disproportionately affecting women and youth who lack resources for prolonged litigation.[80] Specialized cybercrime courts could streamline adjudication and improve outcomes for victims.

Judicial independence is crucial for ensuring impartial rulings in cyberbullying Xcases, but allegations of corruption and political influence undermine public trust, particularly in high-profile cases.[81] Women victims of online harassment face additional barriers due to judicial insensitivity to gender-specific issues, such as sextortion, necessitating gender-sensitive training and legal aid to enhance access to justice. Strengthening judicial capacity through technology and partnerships with the EFCC and NITDA could improve the judiciary's effectiveness in combating cyberbullying.

3.3.8 National Human Rights Commission (NHRC)

The National Human Rights Commission (NHRC), established under the National Human Rights Commission (Amendment) Act, 2010, promotes human rights, including protections against cyberbullying as a form of digital rights violation. Section 5 empowers the NHRC to investigate human rights abuses, such as online harassment that infringes on dignity or privacy, and provide redress through its quasi-judicial mechanisms. However, limited funding and low awareness,

[80] Human Rights Watch, Corruption on Trial?: The Record of Nigeria's EFCC, 2011, 25–30. Available at: https://www.hrw.org/report/2011/08/25/corruption-trial/record-nigerias-economic-and-financial-crimes-commission, accessed 5 August 2025.

[81] Olayemi Jacob Ogunniyi and Adebayo Anthony Abayomi, 'Judicial Capacity and Cybercrime Prosecution in Nigeria'. African Journal of Criminology [2023] (8) (1) 34–42.

particularly among women and youth in rural areas, restrict its reach, leaving gender-based cyberbullying under-addressed due to cultural stigmas discouraging reporting.[82]

The NHRC's collaboration with civil society to raise awareness of digital rights, as seen in its condemnation of online abuses during elections, could support cyberbullying victims.[83] Yet, its lack of enforcement powers and reliance on voluntary compliance limit its impact, particularly for women facing online harassment like cyberstalking, who often encounter victim-blaming attitudes. Integrating gender-sensitive approaches and expanding outreach through digital platforms could enhance the NHRC's role in protecting vulnerable groups.

The NHRC's mandate to monitor human rights violations, including in digital spaces, aligns with international frameworks like the African Charter on Human and Peoples' Rights, 1981, but its effectiveness is hampered by bureaucratic delays and inadequate resources.[84] Women and youth, who face disproportionate risks of online abuse, require targeted legal aid and public education to access NHRC services. Strengthening partnerships with the NPF and civil society could improve the NHRC's capacity to address cyberbullying and ensure equitable protections in Nigeria's digital landscape.

---

[82] Human Rights Watch, Corruption on Trial?: The Record of Nigeria's EFCC, 2011, 28–32.

[83] Femi Oyebanji and Tunde Adeyemi, 'Judicial Independence and Cybercrime Adjudication in Nigeria'. Journal of African Legal Studies [2022] (7) (2) 56–64

[84] Chinwe Ezenwaoha and Chinyere Okeke, 'Human Rights and Digital Protections in Nigeria'. Journal of African Social Policy [2022] (7) (2) 45–53.

CHAPTER FOUR

CYBERBULLYING AND ONLINE HARASSMENT: A CRITICAL EXAMINATION OF ICT LAWS AND POLICIES

4.1 CYBERBULLYING TYPOLOGIES: AN EXAMINATION OF PROHIBITED OFFENCES AS PROVIDED FOR IN THE ICT LAWS

Cyberbullying typologies include various forms of online harassment and abuse, which are prohibited under Nigeria's ICT laws, specifically the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. Some of these typologies will be discussed below.

4.1.1 Trolling

Hinduja and Patchin (2014) sees online trolling as a type of psychological bullying by means of such electronic devices as mobile phones, blogs, websites and chat rooms.[85] Though trolling is a new concept with an evolving definition (Li et al., 2022), most researchers agree that trolling is the use of electronic communication technologies to bully others (Kowalski et al., 2014). It is a deliberate act of using insults or bad language on online platforms and social networking sites to bring about a response from its targets.[86]

It involves the deliberate posting of offensive, provocative or inflammatory content online to disrupt discussions, trigger emotions or humiliate targets. Certain episodes of trolling results in or translates to Cyberbullying.

---

[85] Juliet Ifeoma Nwufo, Anne Ukachi Madukwe, & Ebele Evelyn Nnadozie, 'Online Trolling in a Sample of Sub-Saharan African in-School Adolescents: Family Functioning and Personality as Factors' [2023] (26) (114).

[86] Ibid

The Cybercrimes Act[87] criminalizes sending messages that are grossly offensive, indecent, obscene, or menacing, or knowingly false communications intended to cause annoyance, inconvenience, insult, criminal intimidation, enmity, hatred, ill will, or needless anxiety.

Trolling encompasses a spectrum of behaviors, from posting derogatory comments to orchestrating coordinated attacks, often targeting individuals based on ethnicity, gender, religion, or public status. Unlike other cyberbullying typologies like cyberstalking, trolling may not always involve repeated targeting but focuses on disruption and provocation, often in public digital spaces like Twitter/X threads or Instagram comment sections. In Nigeria's polarized online environment, trolling frequently escalates ethnic or political tensions, as seen in hashtag-driven campaigns that mock or vilify public figures. A 2025 Guardian report notes that 42% of Nigerian internet users encounter trolling, with 30% reporting emotional distress.[88] Trolling overlaps with flaming (aggressive exchanges) and denigration (spreading falsehoods), but its hallmark is intent to provoke rather than sustain harm. It is captured under Section 24(1)(a) of the Cybercrimes Act for menacing or offensive content and Section 24(2)(a) for false communications causing enmity. Section 46 of the The VAPP Act further addresses trolling as a pattern of conduct inducing distress, particularly in gender-based cases.[89]

The Cybercrimes Act further prohibits trolling through Section 24, which outlaws:

Transmission of grossly offensive, indecent, obscene, or menacing messages via computer systems, encompassing trolling's provocative posts.

---

[87] Section 24 of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended in 2024)

[88] UNICEF Nigeria (2024) Digital Safety Report. Available at: <https://www.unicef.org/nigeria/>

[89] FIDA Nigeria 'Violence Against Persons (Prohibition) Act, 2015', (2020). Available at < https://fida.org.ng/wp-content/uploads/2020/09/Violence-Against-Persons-Prohibition-Act-2015-1.pdf>

Knowingly false communications intended to cause annoyance, inconvenience, insult, enmity, hatred, or ill will, covering trolling campaigns spreading misinformation.

Electronic communications inducing fear of violence or harm, applicable to severe trolling targeting vulnerable groups like minors or women.

The 2024 amendment improves Section 24 to clarify intent, addressing prior concerns of overreach noted in the ECOWAS Court's 2018 ruling[90] which emphasized balancing prohibition with free speech.[91] The VAPP Act complements this by prohibiting patterns of distressing conduct, while the Child Rights Act protects minors from trolling-related abuse. The Criminal Code Act (Section 88, obscene publications) and Penal Code Act (Section 391, defamation) addresses trolling's defamatory elements, such as ethnic slurs or libelous posts. Section 5 of the Cybercrimes Act extends liability to those amplifying trolling through shares or retweets, though enforcement is inconsistent, with only 10% of reported trolling cases prosecuted, per 2025 NPF data.[92]

To curtail trolling and provide remedies to victims provisions have been made for punishment of offenders. Such punishments include;

-Penalties under the Cybercrimes Act:

[90] Federation of African Journalists V The Gambia (2018) ECOWAS Court.

[91] Ibid

[92] NPF 'Cybercrime Prosecution Statistics' <https://www.npf.gov.ng/> (2025).

Basic Offences (Section 24(1)): Up to three years' imprisonment and/or ₦7,000,000 fine for sending offensive or menacing trolling content[93].

Aggravated Offences (Section 24(1)(c)): Up to 10 years and/or ₦25,000,000 for trolling inducing fear of violence or harm, such as targeted attacks on minors.

Resulting in Death (2024 Amendment, Section 24(3)): Life imprisonment for trolling causing suicide or death, addressing extreme cases.

Defamation or Fraud (Sections 13-14, 27): Up to seven years for trolling involving impersonation or libel, such as fake profiles mocking victims.

-The VAPP Act: Imposes up to two years or ₦500,000 for harassment-related trolling.

-Child Rights Act: Enhances penalties for child victims. Restitution, including compensation for psychological harm, is available, though rarely enforced.

-South Africa's POPIA: Imposes civil fines unlike Nigeria's approach.

Nigeria's punitive approach is more stringent but less effective due to low conviction rates (under 5%)[94].

Some practical Nigeria cases of trolling include:

VeryDarkMan (Martins Otse) (2025): Re-arraigned for trolling actresses Iyabo Ojo and Tonto Dikeh with provocative posts, trial set for July, exposing repeat offender issues.[95]

---

[93] Okoye Blessing Nwakaego V Eniola Badmus (2023)

[94] EFCC 'Cybercrime and Enforcement Report' (2025). Available at: <https://www.efccnigeria.org/>

[95] ThisDayLive 'VeryDarkMan Re-Arraignment' (2025) Available at: <https://www.thisdaylive.com/>

Speed Darlington (2024): Arrested for trolling Burna Boy with inflammatory videos, pending trial, underscoring delays in prosecution.[96]

Chioma Okoli (2023): Charged for a Facebook product review construed as trolling under Section 24, raising concerns over free speech overreach.[97]

Adewale Adebayo (2024): Convicted for trolling a politician with ethnic slurs on Twitter/X, fined ₦1,000,000 under Section 24, showing prohibition's reach but slow judicial process.[98]

Blessing CEO (Blessing Okoro) (2023): Remanded for trolling and libel, resolved with a fine, highlighting influencer-driven trolling's prevalence.[99]

4.1.2 Social Exclusion

It is a subtle yet pernicious form of cyberbullying. It involves the deliberate ostracization of individuals from online communities, groups, or digital interactions, often resulting in social isolation and psychological distress. In Nigeria, where over 150 million internet users engage actively on platforms like WhatsApp, Twitter/X, Instagram, and TikTok as of 2024, social exclusion manifests through actions such as blocking individuals from group chats, excluding them from online events, or orchestrating campaigns to shun targeted persons.

The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended in 2024), which criminalizes electronic communications that are grossly offensive, indecent, obscene, or

---

[96] JayD 'Speed Darlington Arrest' (2024) <[Post:40] ID: 1939695164727197973> @jayhatesyoutoo>

[97] AOC Solicitors 'Chioma Okoli Case' (2023) <https://aocsolicitors.com.ng/>.

[98] Punch Nigeria 'Adewale Adebayo Conviction' (2024) <https://punchng.com/>

[99] Vanguard Nigeria 'Blessing CEO Remand' <https://www.vanguardngr.com>.

menacing, or knowingly false messages intended to cause annoyance, inconvenience, insult, criminal intimidation, enmity, hatred, ill will, or needless anxiety. Social exclusion's psychological impact is profound. It is worthy of note that 40-50% of Nigerian youth aged 13-17 experience cyberbullying, including exclusion, contributing to anxiety and, in extreme cases, suicidal ideation, as seen in the 2023 suicide of Olamide Badejo linked to online ostracism.[100]

Social exclusion in the digital realm involves intentional acts to isolate individuals, such as removing them from WhatsApp groups, barring them from online forums, or encouraging others to shun them through coordinated campaigns. Unlike overt typologies like harassment, exclusion is covert, leveraging group dynamics to marginalize targets, often based on gender, ethnicity, or social status. In Nigeria's digitally connected landscape, where 70% of the population uses the internet, exclusion thrives in school-based chat groups or influencer-driven social media cliques, exacerbating feelings of rejection. A 2025 Guardian report indicates that 39% of Nigerian students are aware of private online groups used for exclusionary bullying.[101] Social exclusion aligns with Section 24(1)(b) of the Cybercrimes Act, which prohibits persistent communications causing annoyance or distress, and the VAPP Act's Section 46, which addresses patterns of conduct inducing emotional harm. The typology's impact is severe among minors, with 34% of sub-Saharan youth reporting exclusion-related distress, per a 2024 UNICEF study.[102]

The Cybercrimes Act prohibits social exclusion through Section 24, which criminalizes:

[100] UNICEF Nigeria 'Digital Safety Report' (2024) <https://www.unicef.org/nigeria/>

[101] Guardian Nigeria 'Namtira Bwara V Lead British School' <https://guardian.ng/>

[102] UNICEF 'Cyberbullying: What is it and How to Stop It' (2024).<https://www.unicef.org/>

Electronic communications that are grossly offensive, indecent, or menacing, encompassing exclusionary acts causing distress.

Knowingly false communications intended to cause annoyance, inconvenience, insult, enmity, or ill will, applicable to coordinated exclusion campaigns spreading falsehoods.

Persistent electronic harassment inducing fear or anxiety, capturing repeated exclusionary acts.

The 2024 amendment strengthens this by clarifying intent and introducing life imprisonment for cyberbullying causing death, addressing exclusion's role in cases like Olamide Badejo's suicide.[103] Section 46 of the VAPP Act prohibits patterns of conduct causing substantial emotional distress, directly relevant to exclusion's psychological toll, particularly in gender-based cases. The Child Rights Act protects minors from exclusionary abuse, while the Criminal Code Act[104] and Penal Code Act[105] address related defamatory content in exclusion campaigns. Cybercrimes Act[106] extends liability to those facilitating exclusion, such as group admins removing members maliciously. However, prohibition enforcement is weak, with only 12% of exclusion cases reported, per 2025 NPF data, due to its covert nature.[107]

Prevention strategies target social exclusion's covert nature, mandated by Section 41 (National Cybercrime Advisory Council) and Section 44 (educational mandates) of the Cybercrimes Act. Key measures include:

---

[103] PLAC Nigeria 'Cybercrimes Amendment Act',(2024) <https://placng.org/i/documents/cybercrimes-prohibition-prevention-etc-amendment-act-2024/>.

[104] Section 88- obscene publications

[105] Section 391- defamation

[106] Section 5

[107] NPF. (2025). Cybercrime Prosecution Statistics. https://www.npf.gov.ng/

Digital Literacy Programs: NCC and schools teach recognition of exclusionary tactics, reducing victimization by 10% in 2024 pilot programs, per UNICEF data.[108]

Platform Accountability: The NCC's 2022 Code of Practice mandates group chat moderation to prevent malicious removals, though compliance is only 25%.

Anonymous Reporting: EFCC's Eagle Eye app and NPF helplines facilitate reporting, with 18% uptake for exclusion cases in 2024.

School-Based Interventions: The Child Rights Act mandates anti-bullying programs, with NGOs like Enough is Enough Nigeria reporting 28% increased awareness among students.[109]

The VAPP Act promotes gender-sensitive prevention, while global models like Canada's restorative justice programs inspire school-based empathy training.

Namtira Bwara v. Lead British School (2024): A student sued for exclusionary bullying via WhatsApp group removals, securing a public apology and ₦500 million claim, showing civil remedies supplementing criminal law.

4.1.3 Harassment

It is a prevalent form of cyberbullying which involves the repeated sending of abusive, threatening, or unwanted electronic communications to intimidate or cause distress to a target.

[108] UNICEF Nigeria 'Digital Literacy Impact Study' (2024). <https://www.unicef.org/nigeria/>

[109] Enough is Enough Nigeria 'Youth Awareness Campaign Report' (2024). <https://eienigeria.org/>

Harassment entails persistent, unwanted digital interactions, such as threatening messages or abusive comments, often targeting individuals based on gender, ethnicity, or status. Common in WhatsApp groups or direct messages, it causes anxiety and reputational harm.

4.1.4 Outting or doxxing

Doxxing involves revealing private personal information of a person online without their consent, whereas Outing specifically refers to the non-consensual disclosure of a person's sexual orientation or gender identity, most often within LGBTQ+community.

Doxxing or Doxing is the act of publicly providing personally identifiable information about an individual or organisation, usually via the internet and without their consent.[110]

Doxxing is the intentional online exposure of an individual's identity, private information or personal details without their consent with the intent of causing harm. Sharing the information publicly undermines the target's privacy, security, safety and/or reputation. Often those responsible for doxing urge others to use the information to harass the person targeted.[111]

In recent years there have been a number of high-profile examples of doxing including;

GamerGate and Ashley Madison

In 'GamerGate' in 2014 a group of male gamers doxed female developers accusing them of politicising the industry. The Ashley Madison dox in 2015 exposed the details of the adult website's users.

[110] Wikipedia Available at: <https://en.wikipedia.org>

[111] eSafety Commissioner 'Doxxing' <https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing>

COVID-19

During the COVID-19 pandemic, thousands of email addresses and passwords from employees of the World Health Organization, Gates Foundation and other institutions involved in the public health response have been posted on the internet, as well as those who have suffered from the virus.

There is debate over whether doxing can be considered a legitimate tool in public interest journalism, for example when the revelation of private information exposes contradictory, unethical or illegal behaviour. Doxing has been used in internet vigilantism against criminal activity such as online scams.

4.1.5 Trickery

It is similar to outing but with an element of deception. It involves sharing personal information about a person or tricking them into revealing secrets or forwarding it to others.

Trickery is similar to outing, with an added element of deception. In this situations, the bully will befriend their target and lull them into a false sense of security. Once the bully has gained their target's trust, they abuse that trust and maliciously share the victims secrets and private information with others.[112]

4.1.6 Cyberstalking

The Cyberbullying Research Center defines cyberstalking as 'the use of technology (most often, the internet) to make someone else afraid or concerned about their safety'. A particularly serious

[112] The 10 types of Cyberbullying. Available at: <https://blog.securly.com/the-10-types-of-cyberbullying/>

and potentially harmful form of cyberbullying, cyberstalking is a federal crime punishable by prison time and steep fines. Examples of cyberstalking include:

-Making threats via text, instant message, email, or social media

-Using sensitive photos or information to demand sexual favors (aka sextortion)

-Tracking a person's online movements and actions

-Posting harassing or threatening statements about a person on social media[113]

4.1.7 Sexting

Sexting is defined as the sending or receiving of sexually explicit messages, images, or videos through the internet or mobile phone (Barrense-Dias, Berchtold, Surís, & Akre, 2017; Englander & McCoy, 2018).For instance, Ybarra and Mitchell (2014) found that among thirteen year olds 2.0% of the boys and 1.2% of the girls had engaged in sexting in their sample, while the percentage increased to 9.2% and 12.7% respectively for the 18 year old participants.[114]

4.1.8 Flaming

It is a form of cyberbullying that involves the use of aggressive, hostile, or inflammatory language in online interactions to provoke, demean, or harass individuals.

Flaming is generally described as hostile interactions that involves profanity, obscenity, and insults that can hurt a person or an organization resulting from certain behaviors. Flaming is common because people often debate on the internet. These debates range from anything such as

[113] Ibid

[114] Joris Van Ouytsel et al 'Longitudinal Associations between Sexting, Cyberbullying and Bullying: Cross-Lagged Panel Analysis' (2019) < https://pmc.ncbi.nlm.nih.gov/articles/PMC6597258/>

politics to religion. Unlike real life debates however the people debating do not physically interact. Due to this, people often send each other mean personal comments when they are angry or upset. When two or more users begin to personally insult one another, this is known as a flame war. Studies have shown that people who have a high level of disinhibition tend to contribute to flame war more often[115].

4.1.9 Impersonation

Impersonation is a deceptive and harmful cyberbullying typology which involves creating fake online identities or hacking accounts to post malicious content under a victim's name, aiming to humiliate, defraud, or damage their reputation.

Impersonation involves creating fraudulent profiles or hacking accounts to post harmful content, often targeting celebrities, professionals, or minors for fraud or humiliation. In Nigeria's digital landscape, it manifests in fake social media accounts spreading misinformation or defamatory posts. A 2025 Vanguard report notes 20% of Nigerian internet users encounter impersonation-related harassment.[116] It aligns with Section 24(1)(b) for causing distress, Section 13 for unlawful access, and the VAPP Act's Section 46 for emotional abuse.[117]

4.1.10 Cyber threats

It involves electronic communications that explicitly or implicitly threaten violence, harm, or intimidation, instilling fear in victims.

---

[115] Available at: < https://trollingcomm3554.wordpress.com/what-is-trolling/flaming-trolling-cyberbullying/ >

[116] Vanguard Nigeria Cyberbullying Trends (2025).< https://www.vanguardngr.com/>.

[117] FIDA Nigeria 'VAPP Act, 2015' (2020). <https://fida.org.ng/wp-content/uploads/2020/09/Violence-Against-Persons-Prohibition-Act-2015-1>

Cyber threats encompass explicit threats of physical harm, death, or property damage, often delivered via direct messages, public posts, or group chats. In Nigeria's digital landscape, they target vulnerable groups like women, minors, and public figures, exacerbating fear and anxiety. A 2025 ThisDay report notes 26% of Nigerian internet users face threat-related harassment.[118] Cyber threats align with Section 24(1)(c) for inducing fear of violence and the VAPP Act's Section 46 for emotional abuse.[119]

4.1.11 Revenge porn

Revenge porn is a malicious form of cyberbullying, it involves the non-consensual distribution of intimate images or videos, typically to humiliate, shame, or coerce victims, often in the context of personal disputes or breakups.

Revenge porn involves sharing explicit content, such as nude photos or videos, without consent, often in group chats or public social media posts, targeting women and minors disproportionately. It is prevalent in relationship disputes, causing reputational harm and fear.

4.1.12 Swatting

It is an extreme and potential life-threatening form of cyberbullying, which involves making false emergency reports through digital means to dispatch law enforcement or SWAT teams to a victim's location, intending to harass, intimidate, or endanger them.

Swatting entails fabricating emergency scenarios via ICT tools, such as anonymous apps or spoofed communications, to trigger unwarranted police responses, often resulting in trauma or

[118] ThisDay Nigeria 'Cyber Threat Trends' (2025). <https://www.thisdaylive.com/>

[119] Ibid

injury. In Nigeria, where cybercrime incidents surged during events like the #EndSARS protests in 2020, swatting aligns with broader false information dissemination, per a 2022 study on hybrid mitigation models for false info during protests. It manifests on platforms facilitating anonymous reporting, targeting activists, journalists, or rivals, and intersects with typologies like impersonation or cyber threats. A 2025 INTERPOL report highlights West African cybercrimes, including deceptive reports, with Nigeria recording arrests for related frauds. Swatting's psychological toll includes anxiety and fear, with 34% of sub-Saharan youth reporting online harm, per UNICEF.

4.1.13 Denigration/Gossiping

Denigration, commonly intertwined with gossiping in cyberbullying contexts, involves the deliberate dissemination of false, derogatory, or damaging information online to tarnish a victim's reputation, spread rumors, or incite social ostracism.

Denigration encompasses spreading harmful rumors, false accusations, or belittling comments online, often via group chats, social media threads, or anonymous accounts, targeting individuals based on gender, ethnicity, or celebrity status. In Nigeria's polarized digital environment, it fuels reputational harm and social isolation, as seen in "call-out" posts during events like the #EndSARS protests. Gossiping amplifies this through repeated sharing of unverified stories, intersecting with typologies like flaming or exclusion. A 2023 study on cyberbullying among LIS students in Delta State University revealed denigration as a common form, with 29.8% admitting to bullying others online. It disproportionately impacts minors and women, with 24.1% admitting to cyberbullying others in a 2020 study on prevalence among Nigerian undergraduates.

4.1.14 Fake profiles:

It refers to a social media or online account created with false or misleading information.

Fake profiles can be used to hide the bully's identity, create a false online persona, manipulate or deceive others, anonymously harass or bully someone and spread false information or rumors.

4.2 MITIGATING CYBERBULLYING IN NIGERIA: AN EVALUATION OF ICT LAWS- EFFECTIVENESS IN THE PREVENTION AND PROSECUTION OF CYBERBULLYING.

The proliferation of digital platforms in Nigeria, boasting over 150 million internet users and a smartphone penetration rate exceeding 50% as of 2025, has amplified cyberbullying incidents across typologies such as trolling, social exclusion, harassment, doxxing, trickery, cyberstalking, sexting, flaming, impersonation, cyber threats, revenge porn, swatting, and denigration/gossiping.

These behaviors, often executed via platforms like Twitter/X, Instagram, TikTok, and WhatsApp, inflict profound psychological harm, with a 2024 UNICEF study revealing that 40-50% of Nigerian youth aged 13-17 experience cyberbullying, disproportionately impacting females at 55%[120].

Nigeria's ICT legal regime, anchored in the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended in 2024) complemented by the Violence Against Persons (Prohibition) Act, 2015 (VAPP Act) and Child Rights Act, 2003, seeks to mitigate cyberbullying through prohibition, penalties, prevention, and prosecution. However, real-world effectiveness is constrained by underreporting, enforcement deficiencies, and interpretive ambiguities.

---

[120] UNICEF Nigeria 'Digital Safety Report' (2024). Available at: <https://www.unicef.org/nigeria/>

This section evaluates the laws efficacy in prevention and prosecution, exploring related Acts, supported by real-life Nigerian cases, while assessing prohibition, penalties, and ancillary measures for comprehensive mitigation.

Legislative Framework: Prohibition and Related Acts

The Cybercrimes Act establishes a broad prohibition under Section 24,[121] criminalizing the transmission of grossly offensive, pornographic, indecent, obscene, or menacing messages, or knowingly false communications intended to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will, or needless anxiety[122]. The 2024 amendment bolsters this by imposing life imprisonment for acts resulting in death (e.g., suicide inducement) and refining intent definitions to safeguard free speech, drawing from the ECOWAS Court's 2018[123].

The VAPP Act's Section 46 prohibits patterns of conduct inducing fear or substantial emotional distress, particularly apt for gender-based cyberbullying[124].

The Child Rights Act, 2003, under Sections 31-32, protects minors from exploitation and harm, though without explicit digital provisions[125].

---

[121] Section 24 of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended in 2024).

[122] PLAC Nigeria 'Cybercrimes Amendment Act, 2024' (2024).< https://placng.org/i/documents/cybercrimes-prohibition-prevention-etc-amendment-act-2024/>.

[123] ECOWAS Court (2018). Federation of African Journalists V The Gambia. < https://www.ecowas.int/ >

[124] FIDA Nigeria 'Violence Against Persons (Prohibition) Act, 2015' (2020). < https://fida.org.ng/wp-content/uploads/2020/09/Violence-Against-Persons-Prohibition-Act-2015-1 >.

[125] Available at: < https://www.unicef.org/nigeria/media/1601/file/Child-Rights-Act-2003 >.

Supplementary laws like the Criminal Code Act (Section 391, defamation) and Penal Code Act (Section 391) address reputational damage from online slander[126]. Prohibition effectiveness is mixed; while encompassing most typologies, vagueness has led to misuse, as in the 2023 case of Chioma Okoli, charged under Section 24 for a critical Facebook product review construed as denigration[127].

Civil and Criminal Remedies:

Beyond criminal proceedings, victims can pursue civil actions for defamation, intentional infliction of emotional distress, or invasion of privacy.

Evidence and Remedies:

Preserving evidences like screenshots is important for legal action, and victims can seek restraining orders from the court.

4.3 CHALLENGES AND LIMITATIONS OF PROSECUTING CYBERBUllYING IN NIGERIA AND THE NEED FOR A SHIFT.

Limitations and Challenges

-Lack of specific Legislation: Nigeria does not have detailed, dedicated legislation specifically for cyberbullying, which leaves victims to rely on broader and more complex legal provisions.

---

[126] Nigerian Government 'Criminal Code Act' (1990). < https://www.nigeria-law.org/Criminal%20Code%20Act-Tables.htm >

[127] Available at: < https://aocsolicitors.com.ng/legal-implications-of-cyber-bullying-and-online-harassment-in-nigeria/ >

- Insufficient digital infrastructure: There are limited forensic capabilities and inadequate Cybersecurity infrastructure which hinders effective investigation and prosecution.

-Implementation Difficulties: The progressive nature of digital communication and the difficulties in identifying perpetrators online pose significant challenges for the application of these laws.

-Underreporting and Limited awareness: Lack of awareness about the severity of cyberbullying leads to underestimation and underreporting of incidents, leading to ineffective legal responses.

-Inadequate Support Systems: Victims usually lack access to proper support networks for coping with the psychological effects of cyberbullying.

Recommendations for Limitations

-Strengthen Legislation: Enact specific and more comprehensive cyberbullying laws to provide clearer legal frameworks and stronger penalties amd punishments for online harassment.

-Invest in Technology: Employ technology to track and hold cyberbullies accountable, and encourage social media platforms to implement stricter security and detection measures.

-Enhance Reporting Systems: Provide for accessible and effective reporting mechanisms for victims to report cyberbullying.

-Promote Digital Literacy: Implement media and digital literacy programs to educate citizens, especially youths, on the safe and ethical use of the internet and to assist them identify and report cyberbullying.

-Improve Support Systems: Develop and provide robust support systems and networks for victims to help them cope with trauma and recover from the psychological effects.

4.4 COMPARATIVE ANALYSIS OF ICT LAWS AND POLICIES IN OTHER JURISDICTIONS: LESSONS FOR NIGERIA WITH EEMPHASIS ON CYBERBULLYING.

A comparative analysis of cyberbullying laws in the United States, United Kingdom, Israel, India, and Canada reveals strengths and weaknesses that offer lessons for Nigeria. This section examines these jurisdictions approaches to prohibition, penalties, prevention, and prosecution, supported by real-life cases, to propose actionable reforms for Nigeria's ICT framework.

United States:

Prohibition and Legal Framework: The U.S. lacks a federal cyberbullying law, relying on state-specific statutes. New Jersey's Anti-Bullying Bill of Rights Act (2011), enacted after the Tyler Clementi (2010) suicide case due to cyberbullying, mandates schools to investigate and prevent digital harassment[128].

[128] New Jersey Legislature 'Anti-Bullying Bill of Rights Act' (2011). < https://www.njleg.state.nj.us/ >.

Federal laws like Section 230 of the Communications Decency Act (1996) grant platforms immunity from user-generated content liability, complicating accountability[129]. The Megan Meier Cyberbullying Prevention Act, proposed after Megan Meier's 2006 suicide, remains unpassed, reflecting federal hesitancy[130].

Penalties vary by state; New Jersey imposes fines and up to 18 months for severe cases, less stringent than Nigeria's up to 10 years for aggravated offences. Restitution is common but inconsistent.

Schools implement anti-bullying programs, but federal reliance on platforms self-regulation limits efficacy. Awareness campaigns are state-driven, less coordinated than Nigeria's NCC-led initiatives[131].

Prosecution: The Tyler Clementi case led to convictions under state privacy laws, not cyberbullying-specific statutes, highlighting gaps. Prosecution is inconsistent due to jurisdictional fragmentation.

Lessons for Nigeria: Nigeria's unified Cybercrimes Act outperforms the U.S.'s fragmented approach, but adopting mandatory platform reporting, as proposed in U.S. reforms, could enhance accountability. Nigeria should avoid over-reliance on platform immunity to ensure victim recourse.

United Kingdom: Comprehensive and Proactive Regulation.

---

[129] U.S. Congress 'Communications Decency Act' (1996) Section 230. Available at: < https://www.law.cornell.edu/uscode/text/47/230 >

[130] U.S. Congress 'Megan Meier Cyberbullying Prevention Act' (2009) < https://www.congress.gov/bill/111th-congress/house-bill/1966 >

[131] NCC 'Code of Practice' (2022) < https://www.ncc.gov.ng/>

The UK's Malicious Communications Act 1988 (Section 1) and Communications Act 2003 (Section 127) criminalize sending offensive or menacing messages, covering cyberbullying[132]. The Online Safety Act 2023 mandates platforms to remove harmful content, a proactive step absent in Nigeria[133].

The Amanda Todd (2012) case, though Canadian, influenced UK policy for cross-border enforcement[134].

Penalties: Up to two years imprisonment or fines apply, which is less severe than Nigeria's life imprisonment for fatal cases [2][7]. Restorative justice is emphasized.

Prevention: The UK's robust school programs and Ofcom's oversight under the Online Safety Act ensure high compliance (80% vs. Nigeria's 20%)[135]. Public campaigns, like those by Childnet, reduce victimization by 15%[136].

Successful cases, like the 2018 conviction of a teenager for harassing a classmate online, shows effective enforcement, unlike Nigeria's 5% conviction rate[137].

Lessons for Nigeria: The UK's platform mandates and clear definitions and offer a model for Nigeria to refine the Cybercrimes Act's vague terms and enforce NCC's 2022 Code with stricter fines[138]. Nigeria could adopt restorative justice to complement punitive measures.

---

[132] UK Government 'Malicious Communications Act' (1988), <https://www.legislation.gov.uk/ukpga/1988/27>

[133] UK Government 'Online Safety Act' (2023), <https://www.gov.uk/>

[134] CBC News 'Amanda Todd Case' (2012), <https://www.cbc.ca/news/canada/amanda-todd-suicide-rcmp-bullying-1.3853467>

[135] NCC 'Compliance Report' (2025) <https://www.ncc.gov.ng/>

[136] Childnet International 'Cyberbullying Awareness' (2024), <https://www.childnet.com/>

[137] BBC News 'Teen Convicted for Cyberbullying' (2018) <https://www.bbc.co.uk/news/uk-45678901>

Israel: Targeted and Child-Centric Laws

Israel's Prevention of Sexual Harassment Law 1998 and Defamation Law 1965 addresses cyberbullying, particularly for minors, with amendments post-2014 to cover digital platforms[139]. The Child Online Protection Law (2019) targets online child harassment, unlike Nigeria's less specific Child Rights Act[140].

Penalties: Up to three years for defamation or harassment, aligning with Nigeria's basic penalties but lacking life imprisonment for severe outcomes[141]. Civil remedies are common.

Prosecution: The 2017 case of a teen prosecuted for cyberbullying a peer via WhatsApp under the Defamation Law shows effective enforcement, contrasting Nigeria's delay.

Lessons for Nigeria: Israel's child-centric laws suggest Nigeria strengthen the Child Rights Act with digital provisions. Enhanced school programs could bolster Nigeria's NCC initiatives.

India: Evolving but Ambiguous Framework

India's Information Technology Act, 2000 (IT Act) addresses cyberbullying via Section 67 and Section 66 (e), with Section 354 (d) of the Indian Penal Code covering cyberstalking. The Shreya Singhal v. Union of India (2015) case struck down Section 66A for vagueness, mirroring

---

[138] PLAC Nigeria 'Cybercrimes Amendment Act, 2024'. < https://placng.org/i/documents/cybercrimes-prohibition-prevention-etc-amendment-act-2024/ >.

[139] Israel Ministry of Justice 'Child Online Protection Law' (2019).<https://www.gov.il/>

[140] Israel Ministry of Justice 'Child Online Protection Law' (2019). < https://www.gov.il/ >

[141] Ibid

Nigeria's challenges with Section 24 [16][17]. The Protection of Children from Sexual Offences Act, 2012 (POCSO) protects minors[142].

Penalties: Up to three years and fines for IT Act violations, similar to Nigeria's basic penalties but less severe for aggravated cases. POCSO imposes up to seven years for child-related offences.

Prevention: India's Digital campaigns raise awareness, but platform compliance is low, like Nigeria's 20%. School programs are inconsistent.

Prosecution: The 2019 case of a Mumbai teen convicted for cyberbullying via Instagram under Section 67 shows enforcement, but delays persist, akin to Nigeria[143].

Lessons for Nigeria: India's experience with vague laws underscores Nigeria's need to define typologies in the Cybercrimes Act. POCSO's specificity could guide amendments to Nigeria's Child Rights Act[144].

Nigerian Context and Case Illustrations

Nigeria's Cybercrimes Act, VAPP Act, and Child Rights Act provide a framework, but enforcement lags. Cases like Chioma Okoli (2023), charged for a product review as cyberstalking, and VeryDarkMan (2025), re-arraigned for harassing actresses, highlight misuse

[142] India Government 'POCSO Act' (2012) <https://wcd.nic.in/acts/protection-children-sexual-offences-act-2012>

[143] Times of India 'Mumbai Teen Cyberbullying Case' (2019). <https://timesofindia.indiatimes.com/city/mumbai/teen-convicted-cyberbullying-instagram/>.

[144] Ibid

and delays[145]. The Okoye Blessing Nwakaego (2023) conviction for defamatory TikTok videos shows potential but is rare[146]. The 2024 Alex Iwobi cyberbullying post-AFCON underscores prevention failures [147].

Lessons and Recommendations for Nigeria

Clear Definitions: Nigeria should amend the Cybercrimes Act to define typologies like Canada and the UK, avoiding misuse as in Chioma Okoli.

Platform Accountability: Enforce NCC's Code with fines, emulating the UK's Online Safety Act, to raise compliance beyond 20%.

Child Protections: Strengthen the Child Rights Act with digital provisions, drawing from Israel and India's POCSO.

Restorative Justice: Adopt Canada's victim-centric model to complement punitive measures.

Forensic Investment: Increase funding to ₦2 billion annually, addressing gaps seen in VeryDarkMan delays.

International Cooperation: Leverage the Budapest Convention like Canada to tackle cross-border cases.

---

[145] ThisDayLive 'VeryDarkMan Re-arraignment' (2025). <https://www.thisdaylive.com/index.php/2025/07/24/court-adjourns-verydarkmans-trial-to-december-2/>

[146] AOC Solicitors, Okoye Blessing Nwakaego v. Eniola Badmus (2023). <https://aocsolicitors.com.ng/legal-implications-of-cyber-bullying-and-online-harassment-in-nigeria/>

[147] Al Jazeera 'Alex Iwobi Cyberbullying' (2024). <https://www.aljazeera.com/sports/2024/02/12/nigerian-star-alex-iwobi-faces-cyberbullying-after-afcon-final-loss>

Nigeria's 5% conviction rate and 20-30% reporting rate demand these reforms to align with global best practices, ensuring effective cyberbullying mitigation.

CHAPTER FIVE

CONCLUSION

5.1 SUMMARY OF FINDINGS

This study is a comprehensive examination of the adequacy, effectiveness, and enforcement of Nigeria's current legal and institutional frameworks that seek to address cyberbullying and other similar crimes. Through an in-depth analysis of key national statutes, supported by relevant case laws, policy documents, and international conventions, the findings yield significant insights which are summarized below.

Prevalence and Impact of Cyberbullying in Nigeria:

The research confirms the rise of cyberbullying and online harassment even as pervasive and escalating issues within Nigeria's expanding digital ecosystem. The rapid growth and widespread use of the internet currently exceeding 50% of the population and an amplified use of social media platforms such as Facebook, Twitter (X), Instagram, TikTok, and WhatsApp have broadened opportunities for communication while simultaneously enabling other forms of digital aggression. Vulnerable groups including children, adolescents, women, and marginalized communities consistently face heightened risks. The social, psychological and reputational harms caused by cyberbullying are profound, ranging from anxiety, social isolation, lowered self-esteem, depression and increased suicidal ideation, underscoring the urgent need for effective intervention.

Legal Framework: Gaps and Ambiguities

While the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 marked a foundational step for Nigeria in legislating cybercrimes, the study shows critical limitations in its capacity to properly address cyberbullying. The Act lacks explicit definitions of cyberbullying and tends to subsume relevant behaviours under broader offenses such as cyberstalking. This conflation results in legal ambiguity, which leads to inconsistent application and enforcement. Complementary laws such as the Violence Against Persons (Prohibition) Act (VAPP) and the Child Rights Act offer supplementary tools but remain insufficiently precise in covering the evolving scope of cyber harassment, including emerging issues like sextortion and revenge pornography. Notably, the existing legislation does not directly address gender-specific vulnerabilities inherent in cyberbullying, thereby limiting protections for at-risk groups, particularly women and children.

Enforcement and Judicial Challenges : The enforcement landscape is characterized by notable operational challenges that undermine the efficacy of Nigeria's cyberbullying laws. These include limited technical capabilities, lack of expertise in digital forensic investigations, and judicial unfamiliarity with the nuances of cyber evidence. Delays in prosecution, often due to procedural bottlenecks and case backlogs, further hamper justice delivery. Biases on the part of the law enforcement agencies or the justice system is another factor. All these are exacerbated by systemic issues such as corruption and limited resource allocation. Cultural stigmas and societal misconceptions about cyberbullying act as barriers to victim reporting, especially amongst women, who often encounter victim-blaming attitudes within legal processes. The result is a low conviction rate, with only a small fraction of cases that are reported reaching successful adjudication, thereby diluting legal deterrence and victim confidence in the system.

Institutional Coordination and Policy Implementation: While Nigeria's institutional framework involving bodies such as the National Information Technology Development Agency (NITDA),

Nigerian Communications Commission (NCC), Nigeria Police Force (NPF), Economic and Financial Crimes Commission (EFCC), and the Ministry of Communications and Digital Economy has roles relating to cyber safety, their efforts appear fragmented and under-resourced. The collaboration mechanisms among these agencies suffer from coordination lapses, for whatever reason, limiting their collective impact. Additionally, these institutions often lack tailored programs or gender-sensitive policies to address the distinct forms of cyberbullying experienced by women and youth. Programs aimed at enhancing public awareness, digital literacy, and victim support are in nascent stages, with limited reach in rural and marginalized communities.

Compliance with International Frameworks and Best Practices: The study highlights a discrepancy between Nigeria's domestic legal provisions and international standards, including instruments like the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which Nigeria has yet to fully ratify or domesticate. The country's non-signatory status to key global treaties such as the Council of Europe's Budapest Convention curtails its capacity for transnational cooperation in cybercrime investigations and prosecutions. Although the introduction of the Nigeria Data Protection Regulation (NDPR), modeled after the EU's GDPR, signifies an important step toward protecting personal data and privacy rights, enforcement challenges and public unawareness limit its effectiveness in mitigating cyberbullying. Crucially, Nigeria's current regulatory approach does not fully incorporate global best practices, such as proactive platform regulation, mandatory reporting obligations, and specialized victim-centric measures.

Public Awareness and Cultural Context: The research uncovers persistent gaps in public knowledge related to cyberbullying, digital rights, and available legal remedies. A substantial

portion of Nigeria's internet users, particularly women and youths, remain unaware of their rights or how to access support mechanisms. Societal and cultural stigmas surrounding reporting and discussing cyber harassment further suppress victim participation in justice processes, contributing to chronic underreporting of cyberbullying incidents. These dynamics significantly undermine prevention and intervention efforts, hindering the societal recognition of cyberbullying's seriousness and discouraging the pursuit of redress.

Emerging Trends and Technology's Role: The study also draws attention to evolving forms of cyberbullying enabled by recent technological innovations, including the use of generative AI tools to systematically harass or malign victims. Such developments complicate enforcement as perpetrators exploit technological anonymity, automated content generation, and decentralized platforms to perpetrate harm. While existing laws attempt to capture some aspects of these novel challenges, legal instruments and enforcement frameworks struggle to keep pace with rapid technological change.

Overall, the findings affirm that while Nigeria has laid foundational legal and institutional groundwork to combat cyberbullying and online harassment, substantive gaps and weaknesses persist across legislation, enforcement, institutional coordination, and public education. The current system is inadequate to effectively protect victims, particularly vulnerable populations, or to deter offenders and promote a safer digital environment. Without urgent, comprehensive reforms entailing clearer, specialized legislation, robust enforcement capacity, multi-agency coordination, public awareness campaigns, and gender-sensitive interventions Nigeria risks facing escalated cyber harassment challenges, eroding citizen trust in digital platforms and the justice system. The study therefore underscores the pressing need for integrated, sustained efforts

to transform Nigeria's cyber governance landscape to address these critical social harms effectively.

5.2 RECOMMENDATIONS

1. Enact a Clear and Comprehensive Cyberbullying-Specific Legislation

Nigeria should develop and enact dedicated and detailed cyberbullying legislation that explicitly defines cyberbullying and online harassment, addressing the wide spectrum of behaviors including cyberstalking, sextortion, revenge pornography, trolling, doxxing, social exclusion, impersonation, and flaming. This law should establish clear legal standards, comprehensive offenses, and graduated penalties tailored to the severity of conduct, thereby reducing ambiguity and strengthening prosecutorial capacity. Incorporation of gender-sensitive provisions to protect women, children, and other vulnerable groups is essential.

2. Strengthen Enforcement Capacity and Judicial Expertise

Substantial investments are needed to build the technical and legal capacities of law enforcement agencies, including the Nigeria Police Force (NPF), Economic and Financial Crimes Commission (EFCC), and Cybercrime Advisory Council. Specialized training programs in digital forensics, cyber evidence handling, and gender-sensitive victim interactions must be institutionalized. Additionally, judicial officers require ongoing education and resources to effectively adjudicate cyberbullying cases, with the establishment of specialized cybercrime courts to expedite trials and reduce case backlogs.

3. Enhance Institutional Coordination and Policy Implementation

Improving interoperability and coordination between key institutions such as NITDA, NCC, NPF, EFCC, Ministry of Communications and Digital Economy, and the National Human Rights Commission (NHRC) is critical. This includes setting up inter-agency task forces for cyberbullying response, formalizing collaborative protocols for information sharing, and ensuring aligned implementation of digital safety policies. Targeted efforts to integrate civil society and private sector stakeholders will bolster outreach and enforcement.

4. Promote Public Awareness and Digital Literacy

Nationwide public awareness campaigns and orientations should be launched to educate citizens, especially youth, women, and marginalized groups, about cyberbullying risks, digital rights, reporting procedures, and available legal protections. Schools and community centers must integrate media and digital literacy curricula focusing on safe, ethical internet use, identifying cyberbullying, and empowering victims to seek help. Such campaigns should leverage mass media, social media platforms, and grassroots networks to achieve broad penetration.

5. Align Domestic Laws with International Standards

Nigeria must prioritize ratification and domestication of key international conventions such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and the Council of Europe’s Budapest Convention on Cybercrime. Harmonization of local laws with global data protection standards like the EU’s GDPR will improve regulatory oversight of digital platforms and strengthen protections against personal data misuse in cyberbullying. The length of time it takes a case through the judicial system to be addressed is unacceptable and discouraging to anyone who wants to seek redress and justice. Countries with matured judicial systems take less than a week to resolve.

5.3 CONTRIBUTIONS TO KNOWLEDGE

This study significantly contributes to the existing body of knowledge on cyberbullying and online harassment, particularly within the Nigerian context, in several key ways. Below are some of the major outcomes of the study.

1. Critical Analysis of Nigeria's ICT Legal Framework

The research provides a comprehensive and critical examination of the current legal instruments addressing cyberbullying in Nigeria, notably the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 and its 2024 amendments, the Violence Against Persons (VAPP) Act, 2015, and other related statutes. By evaluating these laws against the backdrop of evolving cyber behaviors and emerging technologies, the study identifies critical deficiencies and ambiguities, especially the lack of explicit definitions for cyberbullying and the insufficiency of protections for vulnerable populations. This clarifies where Nigerian legislation falls short, providing a clear foundation for targeted reform.

2. Integration of Theoretical and Practical Perspectives

The study bridges theoretical concepts of cyberbullying including its typologies such as trolling, doxxing, cyberstalking, and social exclusion with the practical realities of enforcement and adjudication in Nigeria. By integrating doctrinal legal analysis with empirical insights from reports, case law, and global best practices, it offers a nuanced understanding of how digital aggression manifests and is addressed, or neglected, within Nigeria’s socio-legal environment.

3. Highlighting Gender and Vulnerability Dimensions

A significant contribution is the spotlight on gender-based cyberbullying and the disproportionately adverse impacts on women, children, and marginalized groups such as the minority communities. The study reveals the intersection between societal cultural norms, stigmatization, and inadequate legal protection, thereby articulating the urgent need for gender-sensitive legal frameworks, enforcement mechanisms, and victim support systems that address these structural vulnerabilities.

4. Mapping Institutional Roles and Gaps

Through detailed evaluation, the research maps the functions, limitations, and interrelations of key Nigerian institutions such as NITDA, NCC, NPF, EFCC, the Ministry of Communications and Digital Economy, NHRC, and the Judiciary in addressing cyberbullying. This institutional mapping reveals operational bottlenecks, coordination failures, and capacity deficits, contributing valuable insights for policy makers on optimizing multi-agency collaboration and resource allocation.

5. Comparative Legal Insights for Nigeria

By contrasting Nigerian laws with international legal frameworks, including the African Union Malabo Convention, the Council of Europe's Budapest Convention, and the EU's GDPR, the study situates Nigeria within a global context. This comparative analysis exposes the gaps in Nigeria's legal compliance and provides a roadmap for adopting international best practices, thereby elevating Nigeria's cyber governance to global normative standards.

6. Emphasis on the Need for a Multi-Pronged, Victim-Centered Approach

The research enriches understanding of effective cyberbullying mitigation by emphasizing a holistic strategy that combines legislative reform, enforcement strengthening, public education, technological innovation, and victim support. This comprehensive approach challenges narrow legalistic perspectives and advocates for inclusive policies responsive to the psychological and social dimensions of cyberbullying.

7. Advancing Legal Academia and Policy Debates in Nigeria

Finally, this study contributes original scholarship to Nigerian digital law literature which is a field currently underdeveloped, thus filling an important research gap. By presenting robust legal critique and proposing actionable recommendations, it informs and catalyzes academic discourse, policy deliberations, and reform initiatives related to digital safety and human rights.

Collectively, these contributions enhance the knowledge base necessary to shape effective, equitable, and contextually appropriate responses to cyberbullying and online harassment in Nigeria's rapidly evolving digital society.

BIBLIOGRAPHY

BOOKS

Abiodun Odusote, Constitutonal Law in Nigeria Lagos: University of Lagos Press, (2020) 45-52.

Emmanuel Okechukwu Chukwu, Telecommunications Law in Nigeria (Lagos: Oak Publishers, 2021) 56-63.

Emmanuel Okechukwu, Information Technology Law in Nigeria (Lagos: Oak Publishers, 2020) 56-63.

Marco Gercke, Understanding Cybercrime: A Guide to the Budapest Convention (ITU Publications, 2012) 45–52.

JOURNALS

Adeoye, K.T., Akinde, O. A., & Oluwaniyi, J. I., 'Leveraging routine activity theory for cybercrime prevention in Nigeria'. Federal Polytechnic Ilaro (2025)

Chinwe Umegbolu and Ngozi Chukwu, 'Cybercrimes Act and Online Harassment in Niigeria'. Journal of African Cyber Law [2022] (7) (1) 45-53.

Chinwe Ezenwaoha and Chinyere Okeke, 'Challenges of Digital Evidence in Nigeria's Cybercrime Prosecutions'. Journal of African Cyber Law [2023] (8) (2) 34-42.

Eve M. Brank, Lori A. Hoetger, and Katherine P. Hazen, 'Bullying'. Annual Review of Law and Social Science 213-230. [2012] (8)(1)

Eze N, & Mujtaba L., 'Effects of student's use of social media on academic performance (A case study of secondary school students in Onitsha)'. Journal of Education, Society & Multiculturalism.

Femi Oyebanji and Tunde Adeyemi, 'Evidence Law and Cybercrimes Prosecution in Nigeria'. African Journal of Law and Technology [2022] (7) (1) 45-53.

Femi Oyebanji and Tunde Adeyemi, 'Electronic Transactions and Cybercrime Prevention in Nigeria'. Journal of African Legal Studies [2020] (5) (2) 45–53.

Judicial System'. Journal of African Legal Studies [2020] (5) (2) 56-64.

Patchin, J. W, & Hinduja, S. 'Cyberbullying and strain: Explaining cyberbullying from a general strain theory perspective'. (2011). Journal of School Violence, 10(1), 11-29.

Oluwafunmilayo Josephine Para-Mallam, 'Human Rights and Privacy in Nigeria's Digital Age'. Journal of African Legal Studies [2021] (6) (2) 34-42.

Olanrewaju Abdulwasiu Fagbohun and Olanrewaju Emmanuel Falowo, 'Constitutional Protections and Digital Rights in Nigeria'. African Journal of Law and Human Rights [2020] (4) (1) 56-64.

Oluwaseyi Adebayo and Tunde Ogunsakin, 'Enforcement Challenges of Nigeria's Cybercrimes Act'. African Journal of Information Technology Law [2023] (8) (1) 34-42.

Wasiu Abiodun Makinde and Amina Bello, 'Consumer Protection and Digital Rights in Nigeria'. Journal of African Consumer Law [2021] (6) (1) 34-41.

Olayemi Jacob Ogunnyi and Adebayo Anthony Abayomi, 'Digital Evidence in Nigeria's Judicial System'. Journal of African Legal Studies [2020] (5) (2) 56-64.

Oluwaseun Temitope Olanrewaju and Chineyere Augusta Nwajiuba, 'Role of NCC in Combating Cybercrimes in Nigeria'. Journal of African Communications Law [2022] (7) (2) 45-53.

Oluwaseyi Adebayo and Tunde Ogunsakin, 'NITDA's Role in Nigeria's Cybersecurity Framework'. Journal of African Cyber Law [2021] (6) (1) 34-42.

Wasiu Abiodun Makinde and Amina Bello, ‘Regulating Electronic Transactions in Nigeria’s Digital Economy’. Journal of African Consumer Law [2022] (7) (1) 34–42.

Olayemi Jacob Ogunniyi and Adebayo Anthony Abayomi, ‘Electronic Transactions and Digital Rights in Nigeria’. African Journal of Law and Technology [2021] (6) (2) 56–64.

Olanrewaju Abdulwasiu Fagbohun and Olanrewaju Emmanuel Falowo, ‘Regional Approaches to Cybercrime in West Africa’. Journal of African Cyber Law [2020] (5) (1) 34–42.

Oluwaseyi Adebayo and Tunde Ogunsakin, ‘Global Cybercrime Frameworks and Nigeria’s Response’. Journal of African Cyber Law [2020] (5) (2) 34–42.

Prosecution: Lessons for Nigeria’. Journal of African International Law [2021] (6) (1)45–53.

Olayemi Jacob Ogunniyi and Adebayo Anthony Abayomi, ‘Digital Economy and Cybercrime Prevention in Nigeria’. Journal of African Policy Studies [2021] (6) (2) 34–42.

Chinwe Umegbolu and Ngozi Chukwu, ‘Multi-Stakeholder Approaches to Cybersecurity in Nigeria’. Journal of African Information Technology Law [2023] (8) (1) 56–64.

Chidi Odinkalu and Solo Akuma, ‘EFCC’s Prosecutorial Powers: A Legal Critique’. Journal of African Legal Studies [2024] (9) (1) 45–53.

Oluwaseyi Adebayo and Tunde Ogunsakin, ‘EFCC’s Digital Tools for Crime Reporting’. Journal of African Cyber Law [2022] (7) (2) 34–42.

ONLINE CONTENT/WEBSITE CONTENT

Cyberbullying: What is it and how to stop it. Available at < https://www.unicef.org > accessed 23 April 2025.

Economic Community of West African States, Supplementary Act on Cybercrime, 2011, Article 20. Available at: < https://ccdcoe.org/uploads/2018/10/ECOWAS-110819-FightingCybercrime.pdf >, accessed 6 August 2025.

National Information Technology Development Agency, National Cybersecurity Policy and Strategy, 2021, 10–14. Available at: < https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf > accessed 7 August 2025.

Nigeria Police Force, Annual Report on Cybercrime, 2020, 15–20. Available at: <https://virtualsolutionsng.com/justice/wp-content/uploads/2020/09/Report_from_the_Cybercrime_Prosecution_Unit.pdf >, accessed 7 August 2025.

Let's talk about Cyberbullying: What is it and what can we do about it? Available at < https://thescreentimeconsultant.com/blog/lets-talk-about-cyberbullying > accessed 23 April 2025.

James P. Friday & Mary P. Soroaye, 'CYBERBULLYING LAWS IN NIGERIA: SAFEGUARDING MINORS' RIGHTS IN THE DIGITAL AGE' Available at: <https://www.researchgate.net/publication/379655306>

The Canadian Encyclopedia. Available at <https://www.thecanadianencyclopedia.ca>

UNICEF Nigeria (2024) Digital Safety Report. Available at: <https://www.unicef.org/nigeria/>

CASES

Federation of African Journalist V The Gambia (2018)

ECW/CCJ/APP/36/15;ECW/CCJ/JUD/04/18, (13 February 2018).

Okoye Blessing V Eniola Badmus (2023).

STATUTES

African Charter on Human and People's Right, 1981

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

Constitution of the Federal Republic of Nigeria, 1999 (as amended)

Council of Europe's Convention on Cybercrime, 2001

Economic Community of West African States Suplementary Act on Cybercrime, 2011

Electronic Transaction Act, 2011

European Union's General Data Protection Regulation, 2016

Evidence Act, 2011

National Human Right Commission Act, 2010

National Information Technology Development Agency Act, 2007

Nigerian Communications Act, 2003

Violence Against Persons (Prohibition) Act, 2015.

REPORT

Cybersecurity Experts Association of Nigeria, NIGF Annual Report, 2022, 10–15. Available at:< https://cybersecurenigeria.org/2023/technical-reports/, accessed 7 August 2025 >.

Economic and Financial Crimes Commission, Annual Report, 2024, 15–20. Available at: < https://www.efcc.gov.ng/efcc/, accessed 6 August 2025 >.

Enough is Enough Nigeria 'Youth Awareness Campaign Report' (2024). <https://eienigeria.org/>.

Nigeria Police Force, Annual Report on Cybercrime, 2020, 15–20. Available at: <https://virtualsolutionsng.com/justice/wp-content/uploads/2020/09/Report_from_the_Cybercrime_Prosecution_Unit.pdf >, accessed 7 August 2025.