

**A CRITIQUE OF THE LEGAL REGIME GOVERNING
CYBERBULLYING IN NIGERIA**

BY

EZEH SYLVIA IFUNANYA

GOU/U23/LAW/694

**A LONG ESSAY SUBMITTED TO THE FACULTY OF LAW, GODFREY OKOYE
UNIVERSITY IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE
AWARD OF THE DEGREE OF BACHELOR OF LAWS (LL.B) OF GODFREY OKOYE
UNIVERSITY, ENUGU STATE, NIGERIA.**

SUPERVISOR: DR. PETER ANIEKE

JULY, 2026.

DECLARATION

I, EZEH SYLVIA IFUNANYA, hereby declare that this Long Essay titled “Legal Regime Governing Cyberbullying in Nigeria” is an original work carried out by me in the Faculty of Law, Godfrey Okoye University, under the supervision of Dr. Peter Anieke.

This work has not been submitted either wholly or partially, for any other degree or professional qualification at any other institution of higher learning within and outside Nigeria.

All sources of information and quotations used in this work have been duly acknowledged.

.....

EZEH SYLVIA IFUNANYA

.....

DATE

CERTIFICATION

I, EZEH SYLVIA IFUNANYA, with registration number GOU/U23/LAW/694 hereby certify that this research carried out by me, with the direct and diligent supervision of Dr. Peter Anieke, has been approved by the Faculty of Law, Godfrey Okoye University, Enugu.

Asides from the sources cited and recognised in this research project, this study is an original work and has not been presented in part or in full, for any degree of this university or any other university to the best of my knowledge.

.....	
EZEH SYLVIA IFUNANYA	DATE
STUDENT/RESEARCHER	

.....	
DR. PETER ANIEKE	DATE
PROJECT SUPERVISOR	

.....	
DR. G. O. OMEH	DATE
(Ag. Dean, Faculty of Law)	

.....	
EXTERNAL EXAMINER	DATE

DEDICATION

This project is dedicated to all victims of cyberbullying, cybercrime and cyberattacks whose experiences continue to inspire the pursuit of justice, legal reform, and the protection of human dignity and privacy. It is equally dedicated to every individual seeking a more just and humane legal system.

ACKNOWLEDGEMENT

First and foremost, I give all glory, honour, and thanksgiving to Almighty God, without whom this journey would not have been possible. He remained faithful even when I was inconsistent, carried me through moments when I had lost hope, and continually directed my steps. There were many times I wanted one thing, but God lovingly reminded me, “Ifunanya, I know you want this, but this is the best for you.” Looking back today, I can only thank Him because every redirection was for my good.

My profound gratitude goes to my parents. To my father, thank you for your unwavering financial support and sacrifices throughout this journey. To my mother, thank you for being a true fighter. If there is ever a battle and my mother is in front, then there is no battle. Thank you both for your different but invaluable contributions to making this dream a reality. May God richly bless you.

I am equally grateful for the wonderful friends God blessed me with — Genelle, Ajiako, Yvonne, Kelly, Precious, and Essential. Your love, encouragement, prayers, and support have meant more than words can express. I truly do not know what I would have done without you all.

Finally, I sincerely appreciate everyone who, in one way or another, contributed to the successful completion of this project. May God bless and reward you abundantly.

TABLE OF CONTENTS

CHAPTER ONE.....	3
INTRODUCTION.....	3
1.1 Background of the Study.....	3
1.2 Statement of the Problem.....	6
1.3 Research Questions.....	8
1.4 Aim and Objectives of the Study.....	8
1.5 Scope and Limitations of the Study.....	9
1.6 Significance of the Study.....	10
1.7 Research Methodology.....	11
1.8 Literature Review.....	11
CHAPTER TWO.....	15
CONCEPTUAL AND THEORETICAL FRAMEWORK.....	15
2.1 Conceptual Framework.....	15
2.1.1 The Concept of Cyberbullying.....	15
2.1.2 The Concept of Legal Regime.....	18
2.1.3 The Concept of Cyberspace, Internet and Computers.....	18
2.1.4 The Concept of Social Media.....	20
2.2 Theoretical Framework.....	21

2.2.1 Natural Law Theory.....	21
2.2.2 Legal Positivism.....	22
2.2.3 Historical School.....	23
2.2.4 Relevance of the Theories to the Study.....	25
2.3 Summary of the Chapter.....	26
CHAPTER THREE.....	29
LEGAL AND INSTITUTIONAL FRAMEWORK GOVERNING CYBERBULLYING IN NIGERIA.....	29
3.1 Legal Framework.....	29
3.1.1 Constitution of the Federal Republic of Nigeria 1999 (as amended).....	29
3.1.2 Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended.....	31
3.1.3 Evidence Act 2011.....	33
3.1.4 Violence Against Persons (Prohibition) Act 2015.....	34
3.1.5 Criminal Code Act.....	34
3.1.6 Penal Code.....	35
3.1.7 African Charter on Human and Peoples' Rights.....	35
3.1.8 Universal Declaration of Human Rights and other International Standards.....	36
3.2 Institutional Framework.....	37
3.2.1 The Courts.....	37

3.2.2 Nigeria Police Force and the National Cybercrime Centre.....	38
3.2.3 Attorney-General and Prosecutorial Authorities.....	39
3.2.4 Nigeria Data Protection Commission.....	39
3.2.5 Nigeria Computer Emergency Response Team (ngCERT).....	40
3.3 Appraisal of the Framework.....	40
3.4 Summary of the Chapter.....	41
CHAPTER FOUR.....	43
APPLICATION OF LAW GOVERNING CYBERBULLYING RELATED MATTERS.....	43
4.1 Judicial and Practical Application of the Law in Cyberbullying-Related Matters.....	37
4.2 Forms of Cyberbullying and Acts That May Amount to Cyberbullying.....	40
4.2.1 Threats, Harassment and Intimidation.....	40
4.2.2 Defamatory and False Publications.....	41
4.2.3 Non-Consensual Sharing of Intimate or Private Content.....	41
4.2.4 Impersonation, Fake Accounts and Identity Abuse.....	42
4.2.5 Blackmail, Sextortion and Extortionate Threats.....	42
4.2.6 Financial and Commercial Cyberbullying.....	43
4.2.7 Trolling, Dogpiling and Coordinated Abuse.....	43
4.2.8 Cyberbullying and Minors.....	44
4.3 Freedom of Expression and the Problem of Overcriminalisation.....	45

4.4 Privacy, Anonymity and Investigative Access.....	47
4.5 Consent and Its Limits in Cyberbullying.....	48
4.6 Major Challenges and Controversies in the Existing Legal Regime.....	49
4.6.1 Conceptual Uncertainty.....	49
4.6.2 Vagueness and Risk of Abuse.....	49
4.6.3 Evidential and Technical Difficulties.....	49
4.6.4 Jurisdictional Problems.....	49
4.6.5 Fear, Shame and Underreporting.....	50
4.6.6 Permanent Digital Harm.....	50
4.6.7 Limited Public Awareness.....	50
4.7 Evaluation.....	51
4.8 Summary of the Chapter.....	51
CHAPTER FIVE.....	52
SUMMARY OF FINDINGS, RECOMMENDATIONS AND CONCLUSION.....	52
5.1 Summary of Findings.....	58
5.2 Recommendations.....	58
5.3 Conclusion.....	62
BIBLIOGRAPHY.....	64

TABLE OF CASES

Nigerian Cases

Abacha v Fawehinmi [2000] 6 NWLR (Pt 660) 228

Dickson v Sylva [2017] 8 NWLR (Pt 1567) 167

Federal Republic of Nigeria v Chioma Edoka Okoli (FHC/ABJ/CR/583/2023)

Federal Republic of Nigeria v Okoye Blessing Nwakaego (FHC/L/343C/2023)

Kubor v Dickson [2013] 4 NWLR (Pt 1345) 534

Ransome-Kuti v Attorney-General of the Federation [1985] 2 NWLR (Pt 6) 211

Solomon Okedara v Attorney-General of the Federation (2019) LPELR-47298(CA) / (CA/L/174/18)

Foreign Cases

J.S. v Blue Mountain School District 650 F3d 915 (3d Cir 2011)

TABLE OF STATUTES

African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, Cap A9 Laws of the Federation of Nigeria 2004

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

Criminal Code Act

Cybercrimes (Prohibition, Prevention, etc.) Act 2015

Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024

Evidence Act 2011

Evidence (Amendment) Act 2023

Nigeria Data Protection Act 2023

Penal Code Law

Police Act 2020

Violence Against Persons (Prohibition) Act 2015

International Instruments

African Charter on Human and Peoples' Rights

Convention on the Rights of the Child 1989

International Covenant on Civil and Political Rights

Universal Declaration of Human Rights 1948

ABSTRACT

This study analyzes the legal framework regulating cyberbullying in Nigeria amidst the growing prevalence of digital interaction and the corresponding escalation of online abuse. Cyberbullying, while not explicitly delineated in Nigerian law, is evidenced by behaviors including harassment, intimidation, threats, impersonation, and the distribution of harmful or misleading information through electronic mediums. The study examines the degree to which current legal frameworks effectively address this phenomenon while preserving a balance with constitutionally guaranteed rights. The research utilizes a doctrinal methodology, drawing upon primary sources such as the Constitution of the Federal Republic of Nigeria 1999 (as amended), the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), the Evidence Act 2011, and the Nigeria Data Protection Act 2023, in addition to pertinent judicial authorities and secondary literature. Analytical and constrained comparative methodologies are utilized to assess the efficacy of the Nigerian legal framework. The study finds that even though there are laws that govern behavior related to cyberbullying, the lack of a clear legal definition and the use of broader crimes like cyberstalking make it hard to understand and apply the law. It also shows that there is a natural conflict between protecting basic rights, especially freedom of speech and privacy, and regulating harmful online behavior. Also, practical problems with enforcement, such as anonymity, evidence requirements, and technological limitations, make existing laws less effective. The study finds that the current laws in Nigeria can be used to deal with cyberbullying, but they are still not very good and need to be changed. It suggests that Nigeria's laws be clearer, that judges interpret them better, and that institutions be stronger to make sure that cyberbullying is regulated in a more consistent and fair way.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The growth of ICT have changed the way people talk to each other, do business, and express themselves in today's world. The rise of the internet, cell phones, social networking sites, and instant messaging services in Nigeria has led to the creation of a virtual space where people interact with each other at a rate, scope, and duration that has never been seen before.¹ The internet has thus ceased to be just a technological tool, but rather a significant social space for making contacts, sharing views, marketing businesses, and building identity.²

However, the same digital platforms that enable connection and participation have also created opportunities for abuse. The virtual space has increasingly become a channel for harassment, threats, intimidation, impersonation, blackmail, ridicule, hate speech, revenge pornography, doxxing and sustained hostile communication directed at individuals.³ These acts are commonly described under the broad label of cyberbullying. Although cyberbullying shares some features with traditional bullying, it is in many respects more invasive and enduring because it may occur anonymously, may be replicated endlessly, and may expose the victim to humiliation before a limitless audience.⁴

1 Constitution of the Federal Republic of Nigeria 1999 (as amended), s 39(1).

2 Muhammed Tawfiq Ladan, *Fake News, Cyber Bullying and Hate Speech on Social Media*(Nigerian Institute of Advanced Legal Studies 2023) 1–4.

3 Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, ss 22, 23, 24 and 26.

4 A O Adediran, 'Cyberbullying in Nigeria: Examining the Adequacy of Legal Responses' (2020) *International Journal for the Semiotics of Law* 34(4) 965, 968–972.

The legal significance of cyberbullying lies in the fact that it affects interests already recognised by law, including dignity of the human person, privacy, personal liberty, reputation and psychological well-being.⁵ It also raises difficult questions concerning the proper limits of freedom of expression in the digital age. The challenge for the law is therefore not merely to prohibit harmful online conduct, but to do so in a way that does not unjustifiably suppress legitimate speech, criticism, satire, consumer complaint or political dissent.⁶

In Nigeria, statutory response to harmful online conduct is found principally in the *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015*, which was enacted to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes.⁷ The Act criminalises, among other things, cyberstalking, identity theft and impersonation, child pornography, racist and xenophobic offences, and related forms of online abuse.⁸ In 2024, the Act was amended, including an amendment to section 24 dealing with cyberstalking.⁹ This amendment is important because section 24 is the provision most frequently discussed in relation to cyberbullying and online harassment in Nigeria.¹⁰

Apart from the Cybercrimes Act, other legal instruments are relevant to the regulation of cyberbullying in Nigeria. The Constitution of the Federal Republic of Nigeria 1999 guarantees the privacy of citizens, their homes, correspondence and telephone conversations under section 37, and also guarantees freedom of expression under section 39.¹¹ At the same time, section 45 of the

5 Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 34 and 37.

6 Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 39 and 45.

7 Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 1.

8 *ibid* ss 22–26.

9 Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, ss 1 and 5.

10 S D Ojukwu and O C Agu, 'Legality of the Cybercrimes (Prohibition, Prevention, Etc.) Act as an Instrument for Internet Crimes Control in Nigeria' [2020] *Nnamdi Azikiwe University Journal of Commercial and Property Law* 7(2) 68, 68–70.

11 Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 37 and 39.

Constitution permits laws that are reasonably justifiable in a democratic society in the interest of public order, public morality, public health, public safety, defence, or for the protection of the rights and freedoms of other persons.¹² The implication is that regulation of cyberbullying in Nigeria must constantly navigate the constitutional tension between individual liberty and collective protection.

No less important is the law of evidence. Given that most cyberbullying incidents usually involve evidence in the form of screenshots, chats, emails, call logs, audio-video recordings, and publications on electronic platforms, the prosecution of such crimes will rely to a significant extent on electronic evidence. Section 84 of the Evidence Act 2011 stipulates the parameters under which statements made in documentary evidence produced by computer would be admissible in proceedings before Nigerian courts.¹³ It follows that a thorough examination of the law of cyberbullying in Nigeria cannot ignore the laws of evidence

The coming into force of the Nigeria Data Protection Act 2023 has contributed immensely to the debates surrounding cyberbullying in the country. The principal objective of the Act is the regulation of personal data processing and protection. Nevertheless, it is an affirmation of the importance of privacy, data security, and personal data protection within the digital world of Nigeria.¹⁴ This provision may be pertinent in cases of cyberbullying where personal data is disclosed, private images are circulated, or private messages are published without consent.

In spite of the developments in statutory law in this field, cyberbullying still presents a challenging phenomenon both legally and socially in Nigeria. There have been responses from the law, but whether such responses are adequate, clear, and balanced with respect to constitutional provisions

¹² *ibid* s 45(1).

¹³ Evidence Act, 2011, s 84.

¹⁴ Nigeria Data Protection Act, 2023, long title and s 1.

remains debatable. While some have commended the Cybercrimes Act as an important legal tool in addressing online abuse, there are those who feel that the Act, in certain cases, provides for formulations that can stifle legitimate discourse.¹⁵ This is the context within which the present work will be carried out.

1.2 Statement of the Problem

The issue of cyberbullying appears to be one of the most lasting consequences related to the development of digital communication in Nigeria. However, although the phenomenon becomes more and more prevalent among individuals, there still exist doubts as to the appropriateness of the existing legal measures against such an offense.¹⁶ The first part of the issue is conceptual. The laws of Nigeria do not necessarily use the phrase ‘cyberbullying’; rather, they refer to cyberbullying under wider concepts like cyber stalking, intimidation, harassment, false messages, obscenity, and extortion among others.¹⁷ This gives the impression that although the laws attempt to tackle issues associated with cyberbullying, they have not created a proper legal framework for cyberbullying

The second issue relates to the scope of certain statutory descriptions. The definitions of offences set out in section 24 of the Cybercrimes Act have been criticised due to their potential to encompass speech that is more than just abusive; phrases like “grossly offensive”, “annoyance”, “insult”, and “needless anxiety” could be used to describe legitimate communication and, therefore, threaten freedom of expression.¹⁸ There is indeed a contradiction when trying to balance the protection of those being bullied with the freedom of speech that the constitution guarantees. A state cannot

15 Adediran (n 4) 975–980; Ojukwu and Agu (n 10) 69–70.

16 Adediran (n 4) 966–968.

17 Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 24.

18 *ibid*; Ojukwu and Agu (n 10) 69.

remain unmoved by the scourge of cyberbullying, nor can it regulate for the sake of censorship.¹⁹

The third challenge involves privacy considerations. Cyberbullying increasingly takes place through supposed private forums like encryption-based messaging applications and closed groups or direct messages. Inevitably, this poses serious dilemmas with respect to investigating criminal behavior via electronic means without unduly infringing on constitutionally guaranteed privacy rights.²⁰ Indeed, the dilemma becomes even more troubling in instances where the offensive conduct, although initially targeting only a select few, was subsequently leaked, shared or broadcasted within a much broader public forum.

Further challenges pertain to practical aspects of enforcing digital crimes. Such crimes typically feature the use of anonymity and pseudonyms, cross-border communications, deleted messages, ephemerality and quick reposting.²¹ Where the substance of the laws are in place, this may prove insufficient for dealing with procedural challenges encountered by victims.

In addition to all of this, there is the issue of insufficient local judicial development in regard to cyberbullying. Despite some court rulings under section 24 of the Cybercrimes Act, Nigeria's case law on the matter is still relatively small compared to the growing types of cyberbullying witnessed in the present day.²¹ There is therefore a considerable number of unsettled issues that require judicial clarification, such as the definition of cyberbullying as opposed to defamation, the point of criminal responsibility, the importance of consent, the legitimacy of humor, and the legality of access to information in cybercrime investigations.

¹⁹ Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 39 and 45.

²⁰ *ibid* s 37; Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 38; Nigeria Data Protection Act, 2023.

²¹ Ojukwu and Agu (n 10) 70; Ladan (n 2) 6–10.

²¹ *Solomon Okedara v Attorney-General of the Federation* (2019) LPELR-47298(CA).

It is against this background that this research aims to explore whether or not the existing legal framework sufficiently addresses cyberbullying in Nigeria and how it can be improved further.

1.3 Research Questions

The study is guided by the following research questions:

1. What is the legal framework governing cyberbullying in Nigeria?
2. To what extent does Nigerian law adequately regulate cyberbullying?
3. How does Nigerian law balance the right to privacy and freedom of speech with rules against cyberbullying?
4. What can Nigeria learn from other countries about how to deal with cyberbullying?

1.4 Aim and Objectives of the Study

The aim of this study is to examine the legal regime governing cyberbullying in Nigeria.

The specific objectives of the study are to:

1. Examine the legal framework regulating cyberbullying in Nigeria;
2. Analyse the adequacy of existing Nigerian laws dealing with cyberbullying;
3. Assess the relationship between cyberbullying regulation and the constitutional rights to privacy and freedom of expression; and
4. Draw lessons from selected comparative jurisdictions with a view to suggesting reforms.

1.5 Scope and Limitations of the Study

This study is limited to the legal regime governing cyberbullying in Nigeria. It focuses principally

on the Constitution of the Federal Republic of Nigeria 1999, the *Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended in 2024*, the *Evidence Act 2011*, and the *Nigeria Data Protection Act 2023*, together with relevant judicial authorities and scholarly literature.²²

On the other hand, in relation to the issue of the subject matter of the study, it can be said that the study covers the legal regulations on cyberbullying, including online harassment, intimidation, threats, impersonations, obscene communications and false communications, among others. However, it should be noted that the study does not aim at discussing all types of cybercrimes covered by the law in Nigeria..²³

The study also makes use of a restricted comparative approach by making comparisons from experiences elsewhere only to the extent that such comparisons help point out the advantages or shortcomings of the Nigerian approach. The main emphasis is on Nigerian law. The research was hampered by the lack of Nigerian court cases addressing cyberbullying explicitly as a legal phenomenon. Moreover, since digital misbehavior tends to advance more quickly than laws and precedents, certain real-world examples of cyberbullying can be developed quicker than the relevant laws. But this does not affect the value of the research; instead, it highlights the need for continued academic attention to the field.

1.6 Significance of the Study

Academically, this research is highly important. First, it adds to the existing corpus of literature within Nigeria on cyber laws, digital rights, and internet abuse issues. Cyber bullying is no longer

²² Cybercrimes (Prohibition, Prevention, etc.) Act, 2015; Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024; Evidence Act, 2011; Nigeria Data Protection Act, 2023.

²³ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, Parts III–VIII.

an emerging social phenomenon; it is a significant legal issue, which lies at the crossroad between criminal law, constitutional law, rules of evidence, privacy, and communication regulations²⁴ Therefore, this research is justifiable.

Second, practically speaking, this research is highly relevant. The findings would be invaluable to lawmakers, judges, prosecuting attorneys, defence attorneys, law enforcement agencies, digital rights organizations, educational establishments, and social media users. They would understand the current legal status quo, the uncertainties associated with the laws, and the reasoning behind the proposed reforms. They would realize the importance of proper legal interpretation of cybercrimes so that the abuses are penalized while lawful speech is protected from unnecessary restrictions.²⁵

Lastly, this research would be highly important in highlighting the flaws and weaknesses within the current framework, which must be addressed by relevant stakeholders through policy initiatives and legislative reforms

1.7 Research Methodology

This study adopts the doctrinal method of legal research. Under this method, reliance is placed on primary and secondary legal materials. The primary materials used include statutes, constitutional provisions and judicial decisions relevant to cyberbullying, cyberstalking, privacy, expression and electronic evidence. The secondary materials include textbooks, journal articles, conference papers and other scholarly commentaries on cyber law, constitutional rights and digital regulation.²⁶

The study also adopts analytical and comparative approaches. The analytical approach is used to

²⁴ Adediran (n 4) 965.

²⁵ Constitution of the Federal Republic of Nigeria 1999 (as amended), s 45; *Solomon Okedara v Attorney-General of the Federation* (2019) LPELR-47298(CA).

²⁶ Bethel Uzoma Ihugba, *Introduction to Legal Research Method and Legal Writing*(Malthouse Press 2020) 95–112.

examine the wording, structure and implications of relevant legal provisions, while the comparative approach is employed in a limited way to evaluate how other jurisdictions respond to similar problems. The materials gathered are subjected to content analysis.

1.8 Literature Review

The phenomenon of cyberbullying has increasingly attracted scholarly and legal attention due to the rapid growth of digital communication and social media usage in Nigeria. Although the concept is relatively modern in legal discourse, its underlying elements, harassment, intimidation, defamation, blackmail and emotional abuse—have long been recognised within both criminal law and tort jurisprudence.

One of the earliest broad discussions on cyber law in Nigeria is found in the work of **M T Ladan**, who examined the legal and institutional response to cyber-related offences in Nigeria. Ladan argues that the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 was a major legislative milestone in the regulation of internet-based misconduct, including cyberstalking and digital harassment. According to him, the Act was designed to protect privacy rights, data integrity, and online safety, while also creating a framework for investigation and prosecution of cyber offences.²⁷

Similarly, **F. Eboibi** in his critical exposition of the Nigerian Cybercrimes Act observes that section 24 of the Act, which criminalises cyberstalking and offensive electronic communication, is the principal statutory basis for prosecuting acts that fall within the broader understanding of

27 Muhammed Tawfiq Ladan, *Fake News, Cyber Bullying and Hate Speech on Social Media*(Nigerian Institute of Advanced Legal Studies 2023) 1–12.

cyberbullying. He notes, however, that the wording of the section, particularly phrases such as “*annoyance*,” “*insult*,” and “*needless anxiety*”, is capable of broad interpretation and may lead to tension with the constitutional right to freedom of expression.²⁸

In the same vein, **S. D. Ojukwu and O. C. Agu** examine the legality and constitutional implications of the Cybercrimes Act as an instrument for internet crime control in Nigeria. Their work is particularly useful in highlighting the constitutional friction between cyberbullying regulation and the rights guaranteed under sections 37 and 39 of the Constitution of the Federal Republic of Nigeria 1999 (as amended). They hold that despite the need for legislative measures aimed at preventing online bullying, such measures have to be crafted in a narrow way to prevent any suppression of freedom of expression.²⁹

From the doctrinal perspective, **Bethel Uzoma Ihugba**, who authored the book *Introduction to Legal Research Method and Legal Writing*, points out that cyber offenses should be analyzed not only from a technological but also from a purely legal point of view. They should be examined as wrongs that relate to crimes, laws on evidence, privacy and constitutional law. This approach of the scholar is especially important for this research because of the role played by the evidence in such cases.³⁰

As for the issue of evidence, there are several important works including *Evidence* by **Nwadiolo and Aguda’s** *Law of Evidence in Nigeria*. Although the latter are not related directly to cyberbullying, they provide a doctrinal basis of section 84 of the Evidence Act 2011 and, therefore, help understand how evidence obtained through electronic devices may be used during

28 F Eboibi, ‘A Critical Exposition of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act 2015’ [2019] (5) *DELSU Law Review* 45.

29 S D Ojukwu and O C Agu, ‘Legality of the Cybercrimes (Prohibition, Prevention, Etc.) Act as an Instrument for Internet Crimes Control in Nigeria’ [2020] *Nnamdi Azikiwe University Journal of Commercial and Property Law* 68.

30 Bethel Uzoma Ihugba, *Introduction to Legal Research Method and Legal Writing* (Malthouse Press 2020) 95–112.

prosecution.³¹

Finally, the victim-centered approach is provided by a recently published article called "The Legal Regime of Cyberbully and Victim Protection in Nigeria" written by Lateef Adeleke and Zainab Oluwo, whereby the authors conduct a critical analysis of both the substance of the laws and institutions in place for protecting the victims of cyberbullying in Nigeria. The authors consider the roles played by the Nigerian Police Force, NCC, NITDA and other regulatory agencies, as well as shortcomings in the implementation of the relevant provisions.³²

Other sources of interest beyond Nigerian academic writings include Danielle Keats Citron who has written extensively on cybercrime and particularly on hate crimes in cyberspace in her book 'Hate Crimes in Cyberspace'. Her works provide important insights into the need for the evolution of the law due to the challenges posed by cyber harassment.³³

However, there is a notable lack in the academic literature that can be identified. A significant proportion of the academic writing on cyber abuse or cyber harassment fails to address the issue specifically as one of cyberbullying. Moreover, there is not sufficient consideration of the tension between constitutional freedoms and rights such as privacy and freedom of speech in relation to cyberbullying.

The present research paper attempts to bridge this gap through the use of a doctrinal approach towards analyzing the legal provisions applicable to cyberbullying in Nigeria.

31 M N Nwadialo, *Modern Nigerian Law of Evidence* (University of Lagos Press 1999) 327; Afe Babalola, *Law and Practice of Evidence in Nigeria* (Sibon Books 2001) 214.

32 Lateef Adeleke and Zainab Ayonimofe Oluwo, 'The Legal Regime of Cyberbully and Victim Protection in Nigeria' [2025] *Fountain University Law Journal* 41–52.

33 Muhammed Tawfiq Ladan, *Fake News, Cyber Bullying and Hate Speech on Social Media* (Nigerian Institute of Advanced Legal Studies 2023) 1–12. ([ResearchGate](#))

CHAPTER TWO

CONCEPTUAL AND THEORETICAL FRAMEWORK

2.1 Conceptual Framework

The proper understanding of the key concepts in this study is essential to a coherent examination of the legal regime governing cyberbullying in Nigeria. Since the topic combines elements of criminal law, constitutional law, information technology law and human rights law, some conceptual clarification is necessary in order to establish the scope and intellectual direction of the study. The major concepts requiring clarification are cyberbullying, legal regime, cyberspace, the internet and computers, and social media.

2.1.1 The Concept of Cyberbullying

Cyberbullying is a relatively modern expression used to describe harmful conduct carried out through electronic means of communication. It generally refers to the use of digital technologies such as mobile phones, computers, social networking platforms, emails, websites and messaging applications to harass, threaten, intimidate, humiliate, blackmail, insult or otherwise victimise another person.³⁴ Unlike traditional bullying, cyberbullying is not confined by physical proximity. It may occur at any time, spread rapidly across multiple platforms, be replicated by third parties, and continue long after the original communication has been made.³⁵

³⁴ Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 3–9.

³⁵ Sameer Hinduja and Justin W Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (2nd edn, Corwin 2015) 11–18.

The word is a compound expression made up of “cyber” and “bullying.” In ordinary usage, “cyber” relates to computers, digital systems or computer networks, while bullying connotes repeated aggressive or hostile behaviour intended to hurt, intimidate, degrade or dominate another person.³⁶ When these ideas are combined, cyberbullying may be understood as bullying behaviour occurring through digital technologies or within electronically mediated spaces.

Scholars have defined cyberbullying in a number of ways. Danielle Keats Citron describes online abuse broadly as technology-facilitated conduct that causes significant emotional, reputational and sometimes physical harm to victims.³⁷ Hinduja and Patchin define cyberbullying as wilful and repeated harm inflicted through the use of computers, cell phones and other electronic devices.³⁸ The Black’s Law Dictionary conception is substantially in the same direction, stressing intentional and repeated digital harm.³⁹ The common elements that run through these definitions are the use of electronic means, the infliction of harm, and the targeting of a victim or identifiable subject.

Cyberbullying may manifest in several forms. These include direct threats of violence, repeated abusive messages, dissemination of false or humiliating information, publication of intimate images without consent, identity theft, impersonation, doxxing, exclusion from online communities, trolling, hate speech directed at a specific victim, and coordinated digital

longer limited to desktop computers. It now occurs through smartphones, tablets, laptops, internet-enabled televisions and other digital devices.

³⁶ Bryan A Garner (ed), *Black’s Law Dictionary* (11th edn, Thomson Reuters 2019) 475, 248.

³⁷ Citron (n 1) 10–18.

³⁸ Hinduja and Patchin (n 2) 11.

³⁹ Garner (n 3) 315.

The legal importance of the internet and computers in this study lies in the fact that they provide both the medium and the evidence of cyberbullying. Harmful acts are executed through them, and proof of those acts is usually derived from screenshots, chat logs, email trails, call records, metadata, digital photographs, video recordings and electronic records.⁴⁰ This explains why the admissibility of computer-generated evidence under section 84 of the Evidence Act 2011 is central to the prosecution or proof of cyber-related misconduct.⁴¹

2.1.4 The Concept of Social Media

Social media refers to internet-based platforms that enable users to create, share, comment on and interact with content in real time or near real time.⁴² They include networking platforms, messaging applications, discussion forums, video-sharing sites, image-based applications and microblogging services. Common examples include WhatsApp, Facebook, Instagram, X, TikTok, Snapchat and Telegram.⁴³

Social media has transformed public discourse, commerce and interpersonal relations. It enables expression, association, advocacy and market visibility on an unprecedented scale.⁴⁴ Yet the same features that make social media useful also make it vulnerable to abuse. The speed of dissemination, relative anonymity, algorithmic amplification and viral character of content make it a fertile ground for cyberbullying.⁴⁵ Harmful material may be reposted, screenshotted, archived and circulated beyond the control of both the victim and the original publisher.

Two social media phenomena are particularly relevant to this study. The first is end-to-end

40 Bethel Uzoma Ihugba, *Introduction to Legal Research Method and Legal Writing* (Malthouse Press 2020) 95–112.

41 Evidence Act, 2011, s 84; *Kubor v Dickson* [2013] 4 NWLR (Pt 1345) 534; *Dickson v Sylva* [2017] 8 NWLR (Pt 1567) 167.

42 Andreas Kaplan and Michael Haenlein, 'Users of the World, Unite! The Challenges and Opportunities of Social Media' [2010] (53) *Business Horizons* 59, 60–61.

43 *Ibid*

44 Andrew Murray (n 18) 40–52.

45 Citron (n 1) 21–39.

encryption, a security feature designed to ensure that messages are readable only by the communicating users and not by the service provider or outsiders in ordinary circumstances.⁴⁶ The second is the phenomenon of parody or impersonation accounts, where a false identity is used to imitate another person. While parody may be used legitimately for humour or satire, it may also be deployed maliciously for harassment, ridicule, deception or reputational injury.⁴⁷ Accordingly, social media is not merely a neutral technological medium. It is a legal and social environment that shapes the forms, speed, visibility and consequences of cyberbullying.

2.2 Theoretical Framework

A theoretical framework provides the conceptual lens through which the subject matter of a study is understood and analysed. However, it does not substitute substantive law; instead, it aids in providing a basis for the understanding of the fundamental philosophy behind legal regulation, including the values upheld by the law, as well as its philosophical foundation. For this research, the following legal theories are especially significant: Natural Law Theory, Legal Positivism, The Historical School, and the Computers Are Social Actors

2.2.1 Natural Law Theory

The natural law theory is an important school of jurisprudence. This school argues that laws are not mere commands that emanate from political authority, but that they are somehow related to reason, morality, and justice.⁴⁸ Classical natural law thinkers such as Aristotle, Cicero and Thomas Aquinas maintained that there are objective principles of right and wrong discoverable by reason

⁴⁶ Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) 87–95.

⁴⁷ Wacks (n 16) 36–43.

⁴⁸ N E Simmonds, *Central Issues in Jurisprudence* (4th edn, Sweet & Maxwell 2018) 9–18.

and rooted in human nature or the order of the universe.⁴⁹

Thomas Aquinas famously described law as “an ordinance of reason for the common good, made by him who has care of the community, and promulgated.”⁵⁰ This conception is relevant to Cyberbullying debases the honor of the victim, destroys mental and emotional stability, and might disrupt the peaceful co-existence of the members of the digital community. Natural Law

Theory condemns such acts because they go against reason and the common good⁵¹

Moreover, the doctrine provides sufficient justification for the belief that some rights, including those of dignity, privacy, and personal security, are not entirely reliant on the legislative grace in order to acquire their moral value. Instead, such rights are derived from the intrinsic worth of man himself..⁵² This assertion finds great resonance with constitutional law regarding fundamental rights in Nigeria. For instance, in *Ransome-Kuti v Attorney-General of the Federation*, Hon. Kayode Eso JSC referred to fundamental rights as “rights which exist above and beyond the ordinary law and prior to political society.”⁵³ That statement reflects a natural law orientation in which basic human claims possess a normative priority.

Applied in this research, the theory of natural law serves as the ethical basis on which the banning of cyber bullying is made. Natural law provides the basis on why the law should protect the victim against the humiliation that takes place online, and how legal principles cannot turn a blind eye to the act of cruelty just because it is done using technological means.

49 Lloyd L Weinreb, *Natural Law and Justice*(Harvard University Press 1987) 1–16.

50 Thomas Aquinas, *Summa Theologica* I-II, Q 90, Art 4.

51 Simmonds (n 28) 14–18.

52 Osita Nnamani Ogbu, *Human Rights Law and Practice in Nigeria* (CIDJAP Press 2013) 3–7.

53 *Ransome-Kuti v Attorney-General of the Federation* [1985] 2 NWLR (Pt 6) 211, 230.

2.2.2 Legal Positivism

Legal positivism adopts an entirely different perspective on the issue. It stresses the distinction between law and morality while insisting that the validity of a law lies mainly in its source, and not necessarily its moral character.⁵⁴ According to positivist scholars like John Austin, laws are simply commands by the sovereign enforced by sanctions.⁵⁵ H L A Hart modified this view by stating that laws are based on a system of primary and secondary rules, and that validity in law comes from established criteria within the legal system itself.⁵⁶

The application of legal positivism to the study is self-evident. While a moral assessment of cyberbullying in Nigeria may determine its immorality, it cannot answer the issue of whether or not cyberbullying is a punishable offence. It can only be determined through positive laws, which include the Nigerian Constitution, the Cybercrimes Act, the Evidence Act, data protection laws, and jurisprudence.⁵⁷ Through the positivist approach, the researcher has to find out the law, structure of the law, interpretation of the law, and sanctions created by the law.

This theory is especially useful in analysing section 24 of the Cybercrimes Act. Whatever moral outrage cyberbullying may provoke, the precise scope of legal liability depends on the wording enacted by the legislature and interpreted by the courts.⁵⁸ The positivist perspective therefore promotes doctrinal clarity and guards against vague moralism. It requires the study to anchor its conclusions in legal texts and judicial reasoning rather than mere sentiment.

Nevertheless, positivism also exposes one of the central difficulties in the present legal regime. If

⁵⁴ H L A Hart, *The Concept of Law* (3rd edn, Oxford University Press 2012) 185–212.

⁵⁵ John Austin, *The Province of Jurisprudence Determined* (Prometheus Books 2000) 18–25.

⁵⁶ Hart (n 34) 79–99.

⁵⁷ Constitution of the Federal Republic of Nigeria 1999 (as amended); Cybercrimes (Prohibition, Prevention, etc.) Act, 2015; Evidence Act, 2011.

⁵⁸ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 24.

the statutory language is too broad, vague or indeterminate, the law may become susceptible to abuse or overreach.⁵⁹ In that sense, positivism not only directs attention to the text of the law, but also reveals why precision in drafting is crucial in the regulation of cyberbullying.

2.2.3 Historical School

The Historical School of jurisprudence, associated most prominently with Friedrich Carl von Savigny, views law as the organic product of the life, culture and historical consciousness of a people.⁶⁰ This school posits that law does not emerge in isolation or exclusively through abstract rational design; rather, it evolves incrementally from custom, social practice, and the communal ethos. This theory is pertinent to Nigerian cyberbullying regulation as it underscores the social underpinnings of legal norms. For a long time, Nigerian society has not liked behavior in which the strong take advantage of the weak, make the weak feel bad, or disrupt the peace of the community..⁶¹ Even before digital technology, social norms and common expectations looked down on making fun of people in public, lying about them, and harassing them in a shameful way. The decision to ban similar behavior online can be seen as an extension of older community rules into a new technological space.

The Historical School also helps us understand why cyberbullying can't be thought of as just an abstract or imported idea. The digital form is new, but the wrongs it shows are common in social life: bullying, humiliation, abuse of power, and damage to one's reputation. So, the law's response is not a big change from Nigerian legal culture; it's more of a modern adaptation of old values to new ways of interacting.

59 Solomon Okedara v Attorney-General of the Federation, discussed in contemporary commentary on the constitutionality of section 24.

60 Dennis Lloyd, *Introduction to Jurisprudence*(6th edn, Sweet & Maxwell 1994) 587–601.

61 T O Elias, *The Nature of African Customary Law* (Manchester University Press 1956) 108–125.

All of the aforementioned theories collectively form a sound jurisprudence basis for the research being conducted. The Natural Law Theory helps explain the morality of dignities and rights against digital violence. The Legal Positivism Theory helps ground the research in terms of the legal rules and statutes. Historical School demonstrates that the legal treatment of cyberbullying is based upon certain social values rather than technological innovation.

The above theories, in their totality, prove that legal intervention against cyberbullying in Nigeria is justifiable not only on legal grounds but also on grounds of morality, societal value systems in

the past, and social behavior. The theories thus reinforce the core thesis of this research paper that cyberbullying needs a proper legal approach in the Nigerian context

The chapter has discussed some of the critical concepts and theories pertaining to this research paper. Cyberbullying refers to a case where an individual engages in intimidation, harassment, embarrassment, threat, and abuse via digital methods of communication. Further, it has been illustrated that the legal system of cyberbullying in Nigeria consists not only of laws but also of constitutional laws, statutory laws, evidentiary rules, and institutional procedures.

In addition to that, the study has established that this issue can be approached from more than one jurisprudential perspective. The moral nature of human dignity according to natural law, legality of the law according to legal positivism, the values of society as explained by the Historical School, and the existence of social injury according to CASA.

Thus, all these theoretical backgrounds lay down the foundation for the next chapter where the

actual legal system of cyberbullying will be studied in detail.

CHAPTER THREE

LEGAL AND INSTITUTIONAL FRAMEWORK GOVERNING CYBERBULLYING IN NIGERIA

3.1 Legal Framework

The legal regime governing cyberbullying in Nigeria is not contained in a single enactment. Rather, it is derived from a network of constitutional guarantees, statutory provisions, evidential rules, criminal law norms, and applicable international human rights instruments. Although Nigerian legislation does not create a standalone offence expressly labelled “cyberbullying,” several existing provisions regulate conduct which, in substance, amounts to cyberbullying, cyber harassment, cyberstalking, online intimidation, non-consensual dissemination of private material, and related forms of digital abuse.⁶²

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

The starting point in any legal analysis of cyberbullying in Nigeria is the Constitution of the Federal Republic of Nigeria 1999 (as amended). The Constitution is relevant in two principal respects. First, it protects rights that are often violated by cyberbullying. Secondly, it protects rights that may be invoked by persons accused of online misconduct.

Section 34 guarantees the dignity of the human person and prohibits inhuman or degrading treatment.⁶³ Cyberbullying frequently involves humiliation, persistent harassment, threats to human dignity. The constitutional value of dignity therefore supplies an important normative basis

⁶² Muhammed Tawfiq Ladan, *Fake News, Cyber Bullying and Hate Speech on Social Media* (Nigerian Institute of Advanced Legal Studies 2023) 10–18.

⁶³ Constitution of the Federal Republic of Nigeria 1999 (as amended), s 34.

for legal protection against severe forms of digital abuse.

Section 37 guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.⁶⁴ This provision becomes relevant where cyberbullying involves unauthorised circulation of private chats, revenge pornography, publication of intimate photographs, doxxing, or the unlawful exposure of personal data. It is equally relevant in the investigative context, because the State must balance the need to investigate cyber offences with the constitutional right to privacy.

Section 39 guarantees freedom of expression, including the freedom to hold opinions and to receive and impart ideas and information without interference.⁶⁵ This section is often raised in debates surrounding section 24 of the Cybercrimes Act. The constitutional challenge is that laws directed at cyber harassment must be framed and interpreted in a manner that punishes genuine abuse without suppressing lawful criticism, reportage, satire, consumer complaint or robust political expression.

The Constitution itself recognises that rights are not absolute. *Section 45* permits laws that restrict *sections 37 and 39* where such restrictions are reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health, or for the purpose of protecting the rights and freedoms of other persons.⁶⁶ This provision is central to the legality of anti-cyberbullying measures. It provides the constitutional basis upon which harmful online conduct may be regulated, provided the restriction is proportionate and not arbitrary.

⁶⁴ *ibid* Section 37.

⁶⁵ *ibid* Section 39.

⁶⁶ *ibid* Section 45.

In *Ransome-Kuti v Attorney-General of the Federation*, the Supreme Court emphasised the elevated nature of fundamental rights in Nigeria's legal order.⁶⁷ This authority remains important because any legislative or executive response to cyberbullying must ultimately be reconciled with constitutional rights.

3.1.2 Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended

The *Cybercrimes (Prohibition, Prevention, etc.) Act 2015* is the principal federal legislation dealing with online misconduct in Nigeria. Its long title shows that it was enacted to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes, as well as the protection of computer systems, networks, electronic communications, data and privacy rights.⁸¹

For the purposes of cyberbullying, the most important provision is *section 24*, which addresses cyberstalking and other harmful electronic communications.⁶⁸ Although the Act uses the term cyberstalking rather than cyberbullying, the provision captures many forms of conduct ordinarily described as cyberbullying, including threatening messages, knowingly false communications intended to cause serious harm, and communication that places another in fear of death, violence or bodily harm.⁶⁹

Amendment of the Act in 2024 was extremely significant. Indeed, the law altered *section 24* owing to constant complaints regarding the imprecise nature and abuse potential of its initial language.⁸⁸ While the new legal framework introduces limitations to some of the earlier terms, it is generally considered as a means of making *section 24* more difficult to exploit in order to penalize lawful

⁶⁷ *Ransome-Kuti v Attorney-General of the Federation* [1985] 2 NWLR (Pt 6) 211.

⁸¹ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, long title.

⁶⁸ *ibid* s 24.

⁶⁹ F Eboibi, 'A Critical Appraisal of Nigeria's Cybercrimes Act' [2017] *University of Benin Law Journal* 88, 95–101.

internet communications..⁷⁰ At the same time, section 24 continues to be the crucial legislative element of the Nigerian response to cyberbullying and online harassment

In addition, the court shall have the right to grant a protective order in a proper case.⁸⁵ Such a right is essential in the fight against cyberbullying since such behaviour usually tends to be repetitive

Beyond *section 24*, other provisions of the Act may become relevant depending on the facts. Identity theft and impersonation under section 22 may apply where false profiles or parody accounts are used maliciously.⁸⁶ Child pornography provisions may apply where abusive conduct involves the circulation of explicit material relating to minors.⁷¹ Provisions relating to racist and xenophobic material may also arise where cyberbullying is directed at a person on prohibited discriminatory grounds.⁷²

The importance of the Cybercrimes Act lies not merely in criminalisation, but in the fact that it provides the most direct statutory basis for addressing harmful digital conduct in Nigeria. Its major weakness, however, is that it still does not define cyberbullying as a distinct and self-contained concept. As a result, the regulation of cyberbullying in Nigeria remains derivative, being filtered through broader categories such as cyberstalking, false messages, obscenity, intimidation and impersonation.⁷³

3.1.3 Evidence Act 2011

The Evidence Act 2011 is an indispensable part of the legal framework governing cyberbullying

70 S D Ojukwu and O C Agu, 'Legality of the Cybercrimes (Prohibition, Prevention, Etc.) Act as an Instrument for Internet Crimes Control in Nigeria' [2020] *Nnamdi Azikiwe University Journal of Commercial and Property Law* 68, 69–

71. ⁸⁵ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 24(4)–(6), as amended. ⁸⁶ *ibid* s 22.

71 *ibid* s 23

72 *ibid* s 26

73 Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 21–39.

because most cyberbullying cases depend on electronically generated evidence. Such evidence may take the form of screenshots, chat logs, emails, audio recordings, videos, metadata, social media posts, call logs and digital archives.⁷⁴

Section 84 of the Evidence Act regulates the admissibility of statements contained in documents produced by computers.⁷⁵ This provision has become central to the proof of digital conduct in Nigerian courts. The Supreme Court in *Kubor v Dickson* stressed the need for compliance with section 84 where electronically generated evidence is sought to be tendered.⁷⁶ Likewise, in *Dickson v Sylva*, the court reaffirmed the importance of laying the proper evidential foundation for computer-generated materials.⁷⁷

This framework of evidence is especially important in cyberbullying cases because the evidence of the wrong usually exists in digital form. A legal framework that criminalizes online abuse yet neglects the admissibility of digital evidence would be virtually ineffective. Because of this, the Evidence Act works with the Cybercrimes Act to make prosecution and adjudication possible.

3.1.4 Violence Against Persons (Prohibition) Act 2015

The Violence Against Persons (Prohibition) Act 2015 also helps to make cyberbullying illegal, especially when it leads to emotional, verbal, or mental abuse. Section 14 makes emotional, verbal, and psychological abuse a crime and sets a punishment for those found guilty⁷⁸ Section 46 gives a broad definition of harassment that includes a pattern of behavior that makes someone afraid of harm or lowers their dignity by sending or delivering information repeatedly through letters, email,

⁷⁴ Afe Babalola, *Law and Practice of Evidence in Nigeria* (Sibon Books 2001) 214–220.

⁷⁵ Evidence Act, 2011, s 84.

⁷⁶ *Kubor v Dickson* [2013] 4 NWLR (Pt 1345) 534.

⁷⁷ *Dickson v Sylva* [2017] 8 NWLR (Pt 1567) 167.

⁷⁸ Violence Against Persons (Prohibition) Act, 2015, s 14.

⁹⁵ *ibid* s 46.

text messages, or other means.⁹⁵

These provisions are highly relevant because many cyberbullying cases do not involve physical assault but instead involve repeated emotional abuse, degradation and intimidation through electronic channels. The VAPP Act is therefore doctrinally useful in showing that Nigerian law does not regard violence solely in physical terms.

It should, however, be noted that the VAPP Act applies directly at the federal level to the Federal Capital Territory, while its wider application across Nigeria depends on adoption by individual states.⁷⁹ Nonetheless, its conceptual significance remains strong, especially because it recognises psychological and verbal abuse as legally cognisable harm.

3.1.5 Criminal Code Act

The Criminal Code Act contains provisions that may apply to certain manifestations of cyberbullying, especially where the conduct involves criminal intimidation, threats, obscene publications or defamatory matter. The law of defamation under the Criminal Code is relevant where false and injurious publications are made online against a person.⁸⁰ Likewise, provisions on intimidation and threats may be invoked where the abusive conduct is aimed at compelling, frightening or silencing the victim.⁸¹

The relevance of the Criminal Code lies in the fact that cyberbullying is often not wholly novel in substance. Many of its constituent wrongs, such as intimidation, blackmail, threat and defamation,

79 D D Dodo, 'The Violence Against Persons (Prohibition) Act 2015: A Legislative Intervention against Gender-Based Violence in Nigeria' [2019] *Ahmadu Bello University Law Journal* 120, 126–128.

80 Criminal Code Act, ss 373–375.

81 *ibid* see also provisions on criminal intimidation and related conduct. ⁹⁹ Penal Code Law, relevant provisions on insult, intimidation and defamation.

were already known to criminal law before the emergence of the internet. The digital environment has therefore changed the medium, scale and speed of the abuse more than the essential character of some of the underlying wrongs.

3.1.6 Penal Code

In Northern Nigeria, the Penal Code contains provisions relating to insult, intimidation, criminal force, defamation and related conduct that may become relevant in particular cyberbullying cases.⁹⁹ While the Penal Code was not designed with modern digital platforms in mind, it remains part of the broader legal architecture through which harmful conduct can be addressed, especially in jurisdictions where it applies.

Its importance lies in demonstrating that cyberbullying may engage general criminal law even where a prosecutor chooses not to rely exclusively on the Cybercrimes Act. The substantive wrong may still be characterised through ordinary criminal law concepts adapted to an online setting.

3.1.7 African Charter on Human and Peoples' Rights

The African Charter on Human and Peoples' Rights is a particularly important human rights instrument in Nigerian law because it has been domesticated and is enforceable within Nigeria.⁸² The Charter safeguards dignity, freedom, personal integrity, and the right to access information and articulate opinions in accordance with the law⁸³ These guarantees are pertinent for both victims of cyberbullying and inquiries regarding the boundaries of lawful regulation.

The Supreme Court confirmed that the African Charter applies in Nigeria in the case of *Abacha*

⁸² African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, Cap A9 Laws of the Federation of Nigeria 2004.

⁸³ African Charter on Human and Peoples' Rights, arts 4, 5 and 9.

v. Fawehinmi.⁸⁴ That decision is significant because it reinforces the point that cyberbullying must be approached within a human-rights-sensitive framework. The State may regulate harmful speech, but it must do so in a manner consistent with legally recognised rights and freedoms.

3.1.8 Universal Declaration of Human Rights and other International Standards

Although the Universal Declaration of Human Rights is not a treaty and is not directly enforceable in the same way as domesticated legislation, it remains an important normative instrument. Article 12 protects against arbitrary interference with privacy, family, home or correspondence and against attacks upon honour and reputation.⁸⁵ Article 19 protects freedom of opinion and expression.¹⁰⁴

Similarly, article 17 of the International Covenant on Civil and Political Rights protects privacy, while article 19 protects expression subject to lawful restrictions.⁸⁶ These instruments are important because they illustrate the international human rights balance that modern cyberbullying regulation must maintain. The legal challenge is not just to stop harmful digital behavior, but to do so in a way that is in line with accepted standards of legality, necessity, and proportionality.

3.2 Institutional Framework

Laws by themselves are not enough to stop cyberbullying. Their effectiveness relies on the institutions tasked with prevention, investigation, enforcement, adjudication, and the safeguarding of rights. The courts, the Nigeria Police Force and its National Cybercrime Centre, prosecutorial authorities, and data protection institutions are the most important places in Nigeria that deal with cyberbullying.

⁸⁴ *Abacha v Fawehinmi* [2000] 6 NWLR (Pt 660) 228.

⁸⁵ Universal Declaration of Human Rights 1948, art 12. ¹⁰⁴ *ibid* art 19.

⁸⁶ Bethel Uzoma Ihugba, *Introduction to Legal Research Method and Legal Writing* (Malthouse Press 2020) 95–112.

3.2.1 The Courts

In cases of cyberbullying, the courts are the last place to go for a decision. They decide if investigations are legal, if digital evidence can be used in court, if laws are constitutional, if people who are accused of crimes are guilty, and if victims can get help.⁸⁷

The court's job is very important in cyberbullying cases because digital crimes often involve weighing the rights of different people. If the communication in question is a real threat or just offensive speech, if privacy rights were violated during the investigation, if section 24 of the Cybercrimes Act was used correctly, and if the rules for letting screenshots, chats, or electronic records be used as evidence were followed, a court may have to decide.⁸⁸

In certain situations, the High Court can also be contacted through fundamental rights enforcement proceedings that deal with privacy, dignity, or expression rights. So, the role of the courts goes beyond punishing criminals to overseeing the Constitution.

3.2.2 Nigeria Police Force and the National Cybercrime Centre

The Nigeria Police Force is the main group that stops and catches criminals in Nigeria. The Police Act 2020 says that the Force must, among other things, stop and find crimes and protect the rights and freedoms of all Nigerians.⁸⁹ When cyberbullying is a crime, this broad legal requirement clearly includes looking into it. The National Cybercrime Centre of the Nigeria Police Force is a special division of the police that looks into and handles complaints about cybercrime.⁹⁰ The growth of this field shows that people are beginning to understand that cyber crimes require more technical

⁸⁷ Ibid.

⁸⁸ Evidence Act, 2011, s 84; *Kubor v Dickson*[2013] 4 NWLR (Pt 1345) 534.

⁸⁹ Nigeria Police Force National Cybercrime Centre, official institutional profile.

⁹⁰ Ibid.

knowledge than regular police work. Cybercrime units are very good at digital tracing, recovering deleted files, keeping electronic evidence, and dealing with online complaints.

The police are still the first place many victims go for help. How they respond has a big effect on whether complaints about cyberbullying are taken seriously, handled by people who know what they're doing, and treated with respect for the law.

3.2.3 Attorney-General and Prosecutorial Authorities

The Attorney-General is in charge of enforcing cyberbullying laws through prosecutorial oversight, either at the federal or state level, depending on the crime and where it happened

¹¹⁰⁹¹ It takes legal judgment to charge people with crimes under the Cybercrimes Act and other related laws, especially when the facts raise constitutional issues or make the evidence hard to understand.

Prosecutors should be involved because not all offensive online messages should lead to criminal charges. Prosecutors must exercise careful discretion to distinguish between genuine cyberbullying and trivial insults, legal critiques, or matters more appropriately addressed through civil remedies or platform reporting mechanisms. A mature legal system needs more than just laws against crime; it also needs rules for prosecutors that are responsible.

3.2.4 Nigeria Data Protection Commission

The Nigeria Data Protection Commission, which was set up by the Nigeria Data Protection Act 2023, is an important organization in cases of cyberbullying that involve the misuse, illegal

⁹¹ Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 174 and 211.

sharing, unauthorized processing, or public exposure of personal data⁹² The Commission is in charge of making sure that personal data is protected and that people follow the rules..⁹³

It is most relevant to cyberbullying when it comes to doxxing, revenge porn, posting private photos, revealing personal addresses or contact information, and other forms of online abuse that invade people's privacy. In these cases, the behavior may break not only criminal law but also data protection law and regulatory enforcement. The Commission adds an important privacy-protective aspect to Nigeria's institutional response to digital abuse as a result.

3.2.5 Nigeria Computer Emergency Response Team (ngCERT)

The Nigeria Computer Emergency Response Team (ngCERT) operates within Nigeria's broader cybersecurity architecture and has the mission of promoting a safe, secure and resilient cyberspace.⁹⁴ NgCERT isn't a criminal court or a prosecuting body, but it does help keep the national cyber ecosystem safe and respond to incidents.

It has an indirect but still important connection to cyberbullying. A safer online world is made possible by raising public awareness, being ready for cyberattacks, reporting digital incidents, and coordinating responses. When cyberbullying and hacking, illegal access, device compromise, or the spread of content after a cyber intrusion happen at the same time, organizations like ngCERT may be useful.

The legal and institutional framework regulating cyberbullying in Nigeria possesses both

⁹² Nigeria Data Protection Act, 2023, ss 4–6.

⁹³ Ibid s.5

⁹⁴ Nigeria Computer Emergency Response Team (ngCERT), official mission statement.

advantages and disadvantages. The best thing about it is that Nigeria doesn't have a legal void. Many kinds of digital abuse can be handled by constitutional rights, criminal laws, rules of evidence, and institutional systems. The Cybercrimes Act, the Evidence Act, the VAPP Act, and human rights laws all work together to give people useful legal tools.

But the framework also has problems with being broken up. Cyberbullying has not yet been established and governed as a distinct offense with particular components. Cyberstalking, intimidation, harassment, emotional abuse, defamation, and privacy violation are all words that mean the same thing in the law. This makes it hard to understand and could cause the rules to be enforced differently.

Another issue is how to protect victims while also upholding constitutional freedom. People might not be able to speak their minds if the law is too vague. If it is too narrow, it might not protect victims well enough. The change to section 24 of the Cybercrimes Act in 2024 looks like it will help find a better balance, but how it works in practice will depend a lot on how judges and prosecutors understand it. The ability of law enforcement to enforce laws still depends a lot on their technical skills and how well they respect people's rights. If laws aren't properly investigated, kept, and prosecuted, they might not work as well as they should.

CHAPTER FOUR

APPLICATION OF LAW GOVERNING CYBERBULLYING RELATED MATTERS

Now that we've looked at the ideas and theories behind cyberbullying in the last chapter and the laws and institutions that govern it in Nigeria, we need to critically examine how the law really works. This chapter examines the practical responses of the existing legal framework to cyberbullying, the diverse manifestations of cyberbullying, the increased susceptibility of minors, the tension between the regulation of cyberbullying and freedom of expression, the importance of privacy and anonymity, the question of consent, and the overarching challenges encountered by enforcement. The objective is not merely to reiterate the law, but to evaluate the adequacy, coherence, and equity of the existing system.

To really look into cyberbullying in Nigeria, you have to realize that it is at the crossroads of many different interests that are at odds with each other. The law's goal is to protect people from online harassment, threats, humiliation, extortion, and other harms. On the other hand, the same set of laws must protect rights that are guaranteed by the Constitution, such as free speech, the right to a fair trial, and privacy. The main goal of the analysis is to find out if the Nigerian legal system strikes a fair balance between protecting victims and protecting civil liberties.

4.2 Judicial and Practical Application of the Law in Cyberbullying-Related Matters

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 is the main law in Nigeria that deals with bad behavior online. The law does not, however, list "cyberbullying" as a separate crime. Instead, the law mostly works through cyberstalking and other crimes that are similar to it, which are listed in section 24.⁹⁵ In practice, a lot of things that people think of as cyberbullying are really cyberstalking. There have been good and bad things about this way of saying things. The good

⁹⁵ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 24.

news is that the law already lets people who are hurt online go to court. The bad part is that the limits of liability aren't always clear when it comes to ideas.

People didn't like the first version of section 24 because it used words that weren't clear, like "grossly offensive," "annoyance," "insult," and "needless anxiety."⁹⁶ People who didn't like this kind of language said it could be used against journalists, activists, unhappy customers, bloggers, and regular people who are speaking out in a strong but legal way. The criticism eventually led to changes in the law, and in 2024, section 24 was changed.¹¹⁶ The change is important because it shows that lawmakers understood that the old wording needed to be clearer. The amendment, on the other hand, does not solve all of the problems with how things are interpreted. Now, the courts have to make sure that section 24 is only used against real online abuse and not to stop speech that makes people uncomfortable.

The courts looked at the issue of section 24 in *Okedara v. Attorney-General of the Federation*. The constitutionality of the provision was questioned on several grounds, including its vagueness and its conflict with freedom of expression.⁹⁷

The Court of Appeal dismissed the challenge and upheld the validity of the provision.⁹⁸ The significance of that decision lies in two points. First, it confirms that the State may constitutionally regulate harmful online conduct. Secondly, it leaves unresolved the practical question of where precisely the line is to be drawn in marginal cases. A provision may be valid in principle and yet still be applied oppressively in practice if investigators, complainants or prosecutors stretch it

96 S D Ojukwu and O C Agu, 'Legality of the Cybercrimes (Prohibition, Prevention, Etc.) Act as an Instrument for Internet Crimes Control in Nigeria' [2020] *Nnamdi Azikiwe University Journal of Commercial and Property Law* 68, 69–71. ¹¹⁶ Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, s 5.

97 *Solomon Okedara v Attorney-General of the Federation* (CA/L/174/18).

98 P Ederagobor, 'Section 24 of Nigeria's Cybercrime Act and its Impact on Freedom of Expression' (2025) SSRN Working Paper 1, 8–12.

beyond its proper purpose.

The 2023 case of Okoye Blessing Nwakaego is a good example of how section 24 can be used. Because of rude and threatening posts he made about actress Eniola Badmus online, the Federal High Court in Lagos found him guilty of cyberstalking her⁹⁹ This case is important because it shows that Nigerian courts will punish people who do bad things online that are ongoing, targeted, and clearly abusive. It also shows that cyberbullying is no longer just a theoretical issue in Nigerian law; it is becoming a real problem that the courts are dealing with more and more.

Another well-known case is the prosecution of Chioma Okoli after she wrote a negative review of an Erisco Foods product on Facebook.¹⁰⁰ The issue became controversial because it brought up the difficult question of whether a negative review from a customer, no matter how bad it was, should be seen as cyberstalking. The case sparked a lot of discussion about too many laws, corporate power, the line between honest opinion and malicious falsehood, and the risk of using cyberstalking law to punish regular speech.¹⁰¹ No matter what the outcome of the case is, it brings up a major point of this study: a law against cyberbullying must be clear enough to tell the difference between real harassment and free speech.

The lesson to take away from these cases is that the Nigerian legal system is slowly getting better at dealing with cyberbullying, but not always in the same way. When the facts include clear threats, humiliation, targeted abuse, blackmail, or the malicious sharing of private information, the law is useful. Where, however, the facts involve satire, criticism, public commentary or commercial complaint, the same legal framework can become controversial. This suggests that the problem is

99 *Federal Republic of Nigeria v Okoye Blessing Nwakaego* (FHC/L/343C/2023); Channels Television, 'Court Sentences Lady to Three Years in Prison for Cyberstalking Eniola Badmus' (2 August 2023).

100 *Federal Republic of Nigeria v Chioma Edoka Okoli* (FHC/ABJ/CR/583/2023).

101 Premium Times, 'Court Grants Erisco Tomato Paste Reviewer Chioma Okoli N5 Million Bail' (31 May 2024).

not simply whether Nigeria has a law, but whether the law is framed and used with sufficient doctrinal discipline.

4.3 Forms of Cyberbullying and Acts That May Amount to Cyberbullying

4.3.1 Threats, Harassment and Intimidation

The most obvious form of cyberbullying consists of repeated threats, insulting messages, intimidation and harassment sent through social media, email, text messages or messaging applications. Such conduct may include threats of violence, repeated abuse, degrading language, or messages designed to create fear, panic or humiliation.¹⁰² This form of conduct falls most naturally within *section 24 of the Cybercrimes Act*, especially where the communication places the victim in fear of death, violence or bodily harm.¹²³

The seriousness of this type of bullying lies in its cumulative effect. One rude message may not always be enough to get someone arrested, but getting the same rude message over and over again can cause a lot of mental pain. The law is thus more warranted in cases of persistence, intentionality, and a distinct harmful objective.

4.3.2 Defamatory and False Publications

Another common form of cyberbullying is when someone posts false or hurtful things online that make the victim feel hate, ridicule, contempt, or damage their reputation.¹⁰³ This could mean making up lies, changing pictures, spreading false rumors, saying someone is immoral, or posting

¹⁰² Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 21–39.

¹²³ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 24(2), as amended.

¹⁰³ Criminal Code Act, ss 373–375.

things on social media to hurt someone's reputation. Sometimes, the actions can be both cyberstalking and defamation at the same time.

The law says that not all harmful publications are considered cyberbullying. The law still needs to be able to tell the difference between facts and opinions, truth and lies, and fair comments and malicious ones. A good legal system should punish people who lie on purpose, but it shouldn't make it illegal to call them out for doing so.

4.3.3 Non-Consensual Sharing of Intimate or Private Content

Sharing nude photos, intimate videos, screenshots of private chats, or other private content without the person's permission is one of the worst kinds of cyberbullying. This behavior is especially harmful because it includes shaming, invading privacy, and often forcing someone to have sex. After a romantic relationship ends, in extortion schemes, or as revenge for what someone thinks is disloyalty, it can happen. This is referred to as revenge pornography or image-based sexual abuse in many places.

This kind of behavior clearly breaks section 37 of the Constitution on privacy, section 34's guarantee of dignity, and the Cybercrimes Act and, in some cases, the Violence Against Persons (Prohibition) Act¹⁰⁴. It is one of the best examples of why cyberbullying shouldn't be seen as just online teasing.

4.3.4 Impersonation, Fake Accounts and Identity Abuse

Cyberbullying can also happen when someone pretends to be someone else, uses fake profiles, or makes parody accounts to hurt someone or steal their digital identity to make fun of them, trick

¹⁰⁴ Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 34 and 37; Violence Against Persons (Prohibition) Act, 2015, ss 14 and 46.

them, or ruin their reputation.¹⁰⁵ The legal significance of this lies in the fact that the bully may hide behind anonymity while weaponising the victim's identity against the victim. Depending on the facts, such conduct may engage the identity theft and impersonation provisions of the Cybercrimes Act.¹⁰⁶

Not every parody account is unlawful; parody and satire are recognised forms of expression. The problem arises where the account is used not for humour or commentary, but for deliberate deception, harassment or reputational sabotage.

4.3.5 Blackmail, Sextortion and Extortionate Threats

Cyberbullying sometimes takes the form of blackmail or sextortion, where a person threatens to release intimate material, personal information or embarrassing communications unless the victim pays money, resumes a relationship, or performs some demanded act. This is a very cruel type of digital abuse because it combines invading someone's privacy with forcing them to do something¹⁰⁷

This kind of cyberbullying is especially bad because it makes the victim feel scared, ashamed, and out of control. Even if the threatened material was first shared with the person's permission, the threat to make it public changes the situation into abuse.

4.3.6 Financial and Commercial Cyberbullying

A more recent trend in Nigeria is what could be called financial cyberbullying. This is often done by predatory digital lenders who shame borrowers by contacting their relatives, posting false

¹⁰⁵ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 22.

¹⁰⁶ Ibid

¹⁰⁷ Citron (n 9) 40–52.

notices, or sending degrading messages to other people. Even though this has something to do with debt collection and protecting consumers, the way it is done is clearly bullying. It uses public shame and fear instead of a legal process to get money back. Depending on the situation, this kind of behavior could break privacy laws, consumer protection laws, and the Cybercrimes Act.

4.3.7 Trolling, Dogpiling and Coordinated Abuse

Cyberbullying can happen to one person or a group of people. In the age of social media, one post can cause a lot of anger, insults, abuse from anonymous users, or what is sometimes called "dogpiling." This type of cyberbullying is especially dangerous because the victim is attacked by a whole group of people online, not just one person. The law has a hard time figuring out who is responsible when abuse spreads quickly among many people. But the damage to the victim is usually very bad, no matter how many people are involved.

4.4 Cyberbullying and Minors

Cyberbullying is most likely to happen to kids and teens. They are vulnerable because of their age, emotional growth, social dependence, and the fact that being humiliated online by their peers can have terrible effects on their education and mental health. Cyberbullying of minors may manifest through derision, body shaming, dissemination of humiliating images, exclusion from digital groups, sexual innuendos, threats, or the propagation of malevolent rumors within peer groups or online communities.

For a long time, the law has said that kids need special protection. Article 19 of the Convention on the Rights of the Child says that State Parties must make laws, rules, and policies in the areas of education, social services, and the law to protect children from all types of physical or mental

violence, injury, or abuse.¹⁰⁸ This duty is broad enough to cover cyberbullying and digital violence. Nigerian child protection law and human rights principles advocate for a more robust protective approach concerning minors.

The law should not only see cyberbullying as a free speech issue because it can hurt kids more than adults. Adults may be able to use harsher language and speak out against each other in politics under the law. But when it comes to kids, the most important thing is to keep their dignity, mental health, and overall growth safe. Cyberbullying can make kids less likely to go to school, hurt their self-esteem, make it harder for them to focus, make them feel bad, and in the worst cases, it can make them hurt themselves.

To stop cyberbullying in Nigeria, kids should learn how to use computers, it should be easy for them to report bullying, investigations should be sensitive to kids, and parents and schools should be more aware of the problem. The law against crime isn't enough. A child who has been embarrassed online needs more than just legal help; they also need help with their schoolwork and their mental health.

4.5 Freedom of Expression and the Problem of Overcriminalisation

One of the hardest problems in this field is figuring out how cyberbullying laws and free speech laws work together. According to Section 39 of the Constitution, everyone has the right to free speech, which includes the right to share ideas and facts.¹⁰⁹ In a democratic society, that freedom is necessary for public debate, journalism, satire, artistic expression, and criticism of products. Section 45 also lets a democratic society put reasonable limits on people's rights and freedoms to

¹⁰⁸ Convention on the Rights of the Child 1989, art 19.

¹⁰⁹ Convention on the Rights of the Child 1989, art 19.

protect the rights and freedoms of others.¹¹⁰ Cyberbullying laws work within a constitutional framework that protects free speech but not abusive behavior.

The hard part is telling the difference between cyberbullying that is against the law and rude speech that isn't. This is especially hard now that people talk to each other on social media in sharp, casual, exaggerated, and quick ways. There are some things people say online that are clearly abusive and threatening.

People can be rude, but that doesn't mean they are breaking the law. Some of the other things are still valid opinions, criticism, or satire. If the law doesn't keep these groups apart, it might not be strong enough to protect victims or make speech too illegal.

The argument about whether or not to charge people based on online reviews, critical posts, or political commentary shows how dangerous this is. In a democracy, people shouldn't be able to threaten, blackmail, or scare other people online. But it shouldn't let people use the law to avoid being embarrassed, looked down on by others, or criticized by the market. It is harder to punish someone for a statement that is mostly true, sincerely believed, or clearly an opinion.

Comparative jurisprudence is enlightening. In the case of *J.S. v. Blue Mountain School District*, the United States Court of Appeals said that a student who made a parody profile of a principal who wasn't on campus shouldn't be punished by the school unless it caused a lot of trouble.¹¹¹ The constitutional framework is different from Nigeria's, but the idea is clear: saying something offensive is not automatically punishable just because it is rude or embarrassing. The law must determine if there is actual harm, an unlawful threat, a deliberate falsehood, targeted harassment, or

¹¹⁰ the Federal Republic of Nigeria 1999 (as amended), s 39.

¹¹¹ *ibid* s 45.

any other reason that requires legal action.

This means that section 24 should be read carefully in Nigeria. Just because a powerful person is upset by something someone says doesn't mean it is cyberbullying. There needs to be a clear sign of malicious falsehood, threatening behavior, intimidation, ongoing harassment, serious invasion of privacy, or something similar. Without this kind of discipline, the law against cyberbullying may be used for convenience instead of justice.

4.6 Privacy, Anonymity and Investigative Access

There is a problem when it comes to privacy and cyberbullying. The victim is worried about protecting their privacy, dignity, and safety. The bully could also be trying to stay anonymous or using encrypted channels of communication to avoid being found. The problem is how to protect privacy while still doing a good job of investigating.

Section 37 of the Constitution protects privacy¹¹² This is especially important when cyberbullying includes leaking private messages, posting pictures without permission, doxxing, or using personal information without permission. From the victim's point of view, cyberbullying is most likely an invasion of privacy. But this doesn't mean that someone can use digital privacy to hide abuse.

Anonymity makes it hard for law enforcement to find out who the criminals are because they often use fake names, multiple accounts, overseas web servers, and even temporary phone numbers. But we shouldn't praise anonymity because, while it can protect whistleblowers and other people who are in danger, it can also lead to cruel behavior.

So, the most important thing is to use a balanced approach. If there are good reasons to think that

112 J.S. v Blue Mountain School District 650 F3d 915 (3d Cir 2011).

cyberbullying has happened, there should be laws that allow for an investigation.

4.7 Consent and Its Limits in Cyberbullying

Some people may use the idea of consent to defend or lessen the guilt of people who cyberbully others. Consent is usually an issue when the victim agreed to share their private information or pictures in the first place. For example, you might ask this question: Is it wrong to share private photos or messages if the victim agreed to it?

The answer to this question will always be yes. In general, consent is limited, specific, and narrow. An individual's consent to share private photos with a romantic partner does not encompass permission for those materials to be disseminated on social networks and online communities. The law knows the difference between consensual acts and illegal things that can happen as a result of those acts. It is both unethical and harmful to the individual's right to privacy to think that the first person's consent is the same as the second person's consent.

The principle of *volenti non fit injuria* is inapplicable in instances of betrayal, extortion, and retaliatory publication.

This reasoning can also apply to things that aren't explicitly sexual. Someone who is involved in politics, social issues, or even business does not automatically give permission for cyberbullying to happen. Being seen in public does not mean giving permission for someone to hurt you. You can criticize a famous person, look into a politician, or look into a business.

4.8 Major Challenges and Controversies in the Existing Legal Regime

4.8.1 Conceptual Uncertainty

One clear flaw in Nigeria's legal system is that the law does not define cyberbullying. Cyberstalking and other similar crimes are what the law is mostly based on. This situation brings up a number of problems. The first problem is that not all cyberbullying is the same as cyberstalking, and vice versa. Cyberbullying includes more than just cyberstalking.

4.8.2 Vagueness and Risk of Abuse

Section 24 is still a sensitive clause, even after changes were made. It is important to look closely at any law that limits free speech. Ambiguity allows those in power to use it to punish people who criticize their actions.

4.8.3 Evidential and Technical Difficulties

Cyberbullying happens when people send messages that disappear, delete their social media accounts, create closed forums, use fake names, and share content on other social media sites. The evidence shown can be changed, destroyed, or challenged because it is not verified.¹¹³ Following Section 84 of the Evidence Act means that some safety measures must be taken into account.

4.8.4 Jurisdictional Problems

Abuse that happens online often crosses borders. The victim might be in one state, the person who hurt them in another, the platform server might be outside of Nigeria, and the harmful content might be available to people all over the world. This brings up hard questions about who has the

¹¹³ Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

right to enforce the law, how to work together to do so, and what to do about it. Digital communication that crosses borders puts a strain on traditional territorial criminal law.

4.8.5 Fear, Shame and Underreporting

Victims of cyberbullying often don't tell anyone about it because they are afraid of getting back at the bully, being embarrassed in public, not being believed, getting in trouble with their family, or having the harmful material spread even more. This is especially true when it comes to private pictures, kids, a broken relationship, or social stigma. You can't just look at how many people get arrested to see how good a legal system is. You also need to see if victims feel safe enough to ask for help.

4.8.6 Permanent Digital Harm

It's really mean to cyberbully because it never stops. Screenshots, downloads, reposts, and archives may keep the damage going even after the post that caused it is deleted. A lot of the time, it's not possible to fully restore. The law can punish and stop people, but it can't always fix what they did wrong. This means that it's very important to stop things from happening and do something right away.

4.8.7 Limited Public Awareness

Many victims don't know what their rights are. Many people who do bad things online don't know what the law says will happen to them. People still don't get very good legal education. Laws aren't used enough or used correctly if people don't know about them.

4.9 Evaluation

The laws in Nigeria that deal with cyberbullying aren't perfect, but they do have some good points. There are some things that are really good about it. The Constitution protects privacy and dignity, the law punishes online harassment, digital proof is becoming more common, and there is more and more case law on the subject. The law can do something about serious abuse, as shown by cases like *Okoye Blessing Nwakaego*.¹¹⁴

The regime is still a work in progress, though, and people can still take advantage of it. When section 24 is used in cases that look more like political speech, business criticism, or a disagreement than real cyberbullying, the danger is even worse. The law works best when the behavior is clearly threatening, blackmailing, invading someone's privacy, or lying on purpose. When the behavior is expressive, critical, or not clear, it gets more attention.

The best conclusion is that Nigeria does have a legal system, but it needs clearer doctrinal boundaries, less strict enforcement, better protocols that take victims' needs into account, and more non-criminal interventions like education, school policies, platform collaboration, and digital literacy.

CHAPTER FIVE

¹¹⁴ Evidence Act, 2011, s 84; *Kubor v Dickson* [2013] 4 NWLR (Pt 1345) 534; *Dickson v Sylva* [2017] 8 NWLR (Pt 1567) 167.

SUMMARY OF FINDINGS, RECOMMENDATIONS AND CONCLUSION

5.1 Summary of Findings

This study analyzed the legal framework regulating cyberbullying in Nigeria, contextualized within the swift advancement of information and communication technology, the proliferation of social media platforms, and the growing migration of personal, social, and commercial interactions to the digital realm. The study aimed to delineate the characteristics of cyberbullying, assess the sufficiency of the Nigerian legal framework governing it, evaluate the degree to which the law reconciles cyberbullying with constitutional rights, including privacy and freedom of expression, and derive insights from comparative and human rights-focused viewpoints.

The primary conclusion of this study is that cyberbullying constitutes a valid and significant form of harm in contemporary Nigerian society. The effects are often very deep, even though it doesn't always lead to physical violence right away. The study found that cyberbullying commonly manifests through threats, repeated online harassment, derogatory comments, intimidation, dissemination of false or humiliating information, non-consensual sharing of private content, impersonation, extortion, and coordinated digital abuse.¹¹⁵ The harm caused by these acts includes psychological distress, reputational injury, invasion of privacy, emotional trauma, social exclusion, economic loss, and in extreme cases, self-harm or suicidal ideation.¹¹⁶ The work therefore found that cyberbullying is not a mere social inconvenience, but a legal wrong capable of undermining constitutionally protected values.

Secondly, the study found that Nigeria does not operate in a legal vacuum in relation to

¹¹⁵ Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 21–39.

¹¹⁶ Sameer Hinduja and Justin W Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (2nd edn, Corwin 2015) 11–29.

cyberbullying. There is an existing body of constitutional, statutory, evidential and institutional rules that may be invoked to address the problem. At the constitutional level, sections 34, 37, 39 and 45 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) are of particular relevance.¹¹⁷ Section 34 protects the dignity of the human person; section 37 guarantees privacy of correspondence and communications; section 39 protects freedom of expression; and section 45 permits lawful restrictions on certain rights where reasonably justifiable in a democratic society for the protection of other rights or public interests.¹¹⁸ The study found that these provisions collectively form the constitutional framework within which cyberbullying must be assessed. On the one hand, they support protection against humiliation, privacy invasion and degrading conduct. On the other hand, they caution against legal responses that suppress legitimate speech under the guise of anti-cyberbullying enforcement.

Thirdly, the study found that the principal statute presently dealing with harmful online conduct in Nigeria is the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended.¹¹⁹ The Act does not create an express standalone offence called “cyberbullying.” Instead, most cyberbullying-related conduct is regulated through the offence of cyberstalking and related provisions, especially section 24.¹⁴¹ This section criminalises certain categories of harmful electronic communication, including threatening messages, knowingly false communications intended to cause serious harm, and communication capable of placing another person in fear of death, violence or bodily harm.¹²⁰ The study found that this statutory approach is both useful and limited. It is useful because it gives law enforcement and the courts a basis for punishing harmful online conduct. The law doesn't make it clear what cyberbullying is as a bigger social and legal problem, which makes it hard to

117 Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 34, 37, 39 and 45.

118 *ibid*.

119 Cybercrimes (Prohibition, Prevention, etc.) Act, 2015; Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024.

¹⁴¹ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 24.

120 *ibid*

understand and use all the time.

The fourth finding is that the Cybercrimes Act will be changed in 2024, which is a big step forward for Nigerian cyber law. The change shows that lawmakers are aware that the old wording of section 24 caused a lot of trouble. People thought that words like "annoyance," "insult," and "needless anxiety" were too vague and could be used in bad ways.¹²¹ The study found that the change is an effort to make the law less broad and lower the risk of making free speech illegal.¹²² However, it was also discovered that amendment alone does not rectify all issues. The law still works in practice because judges carefully interpret it, prosecutors are careful not to overreach, and investigators and complainants are sensitive to people's rights.

A fifth conclusion of the study is that evidential law is essential to the efficacy of the legal framework regulating cyberbullying. Most cases of cyberbullying rely on evidence that was made electronically, like screenshots, emails, chat logs, call records, audio-visual materials, metadata, and old digital posts.¹²³ Section 84 of the Evidence Act 2011, as changed in 2023, is the main law that governs the use of such evidence.¹²⁴ The research indicates that the law of evidence is not ancillary to cyberbullying litigation; it is fundamental. Without a functional evidentiary framework, the criminalization of cyberbullying would remain predominantly theoretical. Judicial cases like *Kubor v. Dickson* and *Dickson v. Sylva* show how important it is to have a strong evidential basis when using computer-generated evidence.¹²⁵

The sixth finding is that the Nigerian legal system that deals with cyberbullying goes beyond the

121 D Ojukwu and O C Agu, 'Legality of the Cybercrimes (Prohibition, Prevention, Etc.) Act as an Instrument for Internet Crimes Control in Nigeria' [2020] *Nnamdi Azikiwe University Journal of Commercial and Property Law* 68, 69–71.

122 Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024, s 5.

123 Bethel Uzoma Ihugba, *Introduction to Legal Research Method and Legal Writing* (Malthouse Press 2020) 95–112.

124 Evidence Act, 2011, s 84; Evidence (Amendment) Act, 2023.

125 *Kubor v Dickson* [2013] 4 NWLR (Pt 1345) 534; *Dickson v Sylva* [2017] 8 NWLR (Pt 1567) 167.

Cybercrimes Act. The Violence Against Persons (Prohibition) Act 2015, the Criminal Code, the Penal Code, the African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, and the Nigeria Data Protection Act 2023 are all important laws that help shape the regulatory landscape.¹²⁶ The Violence Against Persons (Prohibition) Act is especially important when there is emotional, verbal, or psychological abuse. The Nigeria Data Protection Act is important when cyberbullying involves the illegal exposure or misuse of personal information.¹²⁷ The study concluded that the Nigerian response to cyberbullying is diverse in legal sources, despite lacking conceptual cohesion.

The seventh conclusion of the study indicates that the institutional response to cyberbullying in Nigeria remains in a state of development. The courts, the Nigeria Police Force, its specialized cybercrime units, prosecutors, and other regulatory bodies all have a part to play¹²⁸ The courts are still very important because they decide if laws are constitutional, explain what they mean, look at evidence, and weigh the rights of both the complainant and the defendant.¹²⁹ However, the study found that the legal system's success depends on more than just the rules of the law. It also depends on the technical skills of law enforcement, the quality of the investigation, the preservation of digital evidence, and how victims are treated.

One of the biggest problems in this area is that rules against cyberbullying and freedom of speech are at odds with each other. The research indicated that this tension is inevitable in a democratic society. Not all harsh, rude, or offensive things said online are cyberbullying. There is a difference between real threats, malicious lies, targeted harassment, blackmail, and behavior that invades

126 Violence Against Persons (Prohibition) Act, 2015, ss 14 and 46; Criminal Code Act, ss 373–375; African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, Cap A9 Laws of the Federation of Nigeria 2004; Nigeria Data Protection Act, 2023.

127 Violence Against Persons (Prohibition) Act, 2015, s 14; Nigeria Data Protection Act, 2023.

128 Police Act 2020, s 4

129 Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 6, 36, 46.

someone's privacy, and lawful criticism, opinion, parody, satire, public commentary, or honest consumer review.¹³⁰ It's true that overcriminalization is a problem. The study discovered that if the law is not carefully interpreted, anti-cyberbullying provisions could be exploited by influential complainants to penalize embarrassment, scrutiny, or dissent instead of actual abuse.

Ninthly, the study discovered that privacy assumes a dual role in cyberbullying discourse. The victim frequently cites privacy as a right infringed upon by doxxing, revenge pornography, the dissemination of private communications, or the revelation of personal information. The perpetrator may also use encryption, anonymity, or privacy claims to avoid being held responsible.¹⁵³ The research revealed that privacy cannot be regarded in absolute terms within this context. The law must protect digital privacy, but it must also allow lawful, reasonable, and targeted investigative access when there are credible claims of cyberbullying that is illegal. The challenge is to make sure that the privacy veil is only lifted when the law says so and not for no reason.

The tenth finding is about the issue of consent. The study determined that consent is pertinent yet constrained. Agreeing to send a private picture or message to one person does not mean that the person agrees to share that picture or message with the public, use it to blackmail someone, or spread it around to humiliate someone.¹³¹ The study thus determined that the maxim *volenti non fit injuria* has limited applicability in cases of cyberbullying. It cannot be extended to justify revenge publication, digital betrayal, or blackmail solely on the basis that the victim initially entrusted the offender with private content. The law must acknowledge the contextual and particular nature of

130 *J.S. v Blue Mountain School District* 650 F3d 915 (3d Cir 2011); Muhammed Tawfiq Ladan, *Fake News, Cyber Bullying and Hate Speech on Social Media* (Nigerian Institute of Advanced Legal Studies 2023) 10–18. ¹⁵³ Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

131 Clare McGlynn, Erika Rackley and Ruth Houghton, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' [2017] *Feminist Legal Studies* 25, 25–46. ¹⁵⁵ Convention on the Rights of the Child 1989, art 19.

consent.

The 11th finding is that kids and other groups that are at risk need more protection. The study found that kids are more likely to be victims of cyberbullying because of their age, emotional development, and social weakness.¹⁵⁵ It also found that the current Nigerian system doesn't do enough to protect women, children, people with disabilities, and people who have been victims of technology-facilitated gender-based violence. Some of these cases can still be protected by existing laws, but the protection is still indirect and not very strong.¹³²

The twelfth thing the study found was that anonymity, fake accounts, and communication across borders make it very hard to enforce the law. Cyberbullies can make it hard to find out who they are by using fake names, temporary numbers, foreign-hosted platforms, or multiple accounts¹³³

Another problem is that digital harm lasts forever. Once harmful content is downloaded, copied, reposted, or archived, it is nearly impossible to restore it completely.¹³⁴ This means that the traditional legal idea of full restoration doesn't always work in cyberspace.

The study found that the main problem with the current Nigerian government is not that there are no laws at all, but that there is no clear, fair, and victim-centered legal framework that deals with cyberbullying. Nigeria has enough laws to step in, but they aren't always clear enough to tell the difference between free speech and cyberbullying, legal investigation and invasion of privacy, and general cybercrime and the specific realities of image-based abuse, online shaming, and technology-facilitated gender violence¹³⁵ The Nigerian legal system works in that way, but it's not perfect.

¹³² *ibid*; Violence Against Persons (Prohibition) Act, 2015.

¹³³ Andrew Murray, *Information Technology Law: The Law and Society* (4th edn, Oxford University Press 2019) 1–14.

¹³⁴ Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge University Press 2014) 87–95.

¹³⁵ F Eboibi, 'A Critical Appraisal of Nigeria's Cybercrimes Act' [2017] *University of Benin Law Journal* 88, 95–101.

5.2 Recommendations

To make the laws clearer, the National Assembly should first consider adding language that clearly defines cyberbullying as a separate legal concept. Section 24 of the Cybercrimes Act is important, but the current law mostly deals with cyberbullying by using the broader term "cyberstalking."¹³⁶ A better-written law should make the crime clearer, list its most important parts, and make it clear that it is not the same as free speech, defamation, parody, or just being annoying. Victims,

investigators, prosecutors, and the courts would all find it easier to understand the law if this change were made.

Second, Nigeria's anti-cyberbullying law should make it clear that privacy, dignity, and freedom of speech are all protected by the Constitution. The law should make it clear that saying something bad about someone, making fun of them, or writing honest reviews of products are not crimes just because they make the person feel bad or embarrassed.¹³⁷ It should also keep harsh punishments for real threats, harassment that doesn't stop, lying, extortion, and sharing private information without permission. This explanation would make it less likely that people will be charged with too many crimes.

Third, the law should make it clear that revenge porn, sextortion, image-based sexual abuse, and technology-facilitated gender-based violence are all wrong. People don't always understand how bad cybercrime is when they hear it called that.¹³⁸ These kinds of abuse can be very bad, especially

¹³⁶ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 24.

¹³⁷ Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 39 and 45.

¹³⁸ McGlynn, Rackley and Houghton (n 19) 25–46.

for women and girls. A clearer answer from the government would help protect victims and show how digital abuse really happens today.

Fourth, the system should do more to keep kids and other groups that are at risk safe. Nigerian law should have reporting procedures that are kid-friendly, stronger anti-cyberbullying rules in schools, and more specific recognition of the unique harm that online humiliation or harassment can do to kids.¹³⁹ Article 19 of the Convention on the Rights of the Child should not just be an idea; it should lead to real protections in schools and the law.¹⁴⁰

Fifth, police should learn more about how to do digital investigations, keep data safe, do cyber-forensics, and deal with complaints that are sensitive to rights.¹⁴¹ There are more problems with cyberbullying than just the law. Another issue is how to properly collect and store evidence. More training would mean fewer cases that don't go to trial, better protection of digital evidence, and more trust in the system by the public.

Sixth, the courts should keep being careful and principled when it comes to section 24 of the Cybercrimes Act. Before a court can find someone guilty of a crime, it should need clear proof of intent, harmful behavior, targeted abuse, malicious falsehood, or illegal threats.¹⁴² This is important so that powerful people can't use anti-cyberbullying laws to make it illegal to criticize or embarrass someone in public.

Seventh, civil and protective remedies should be used more often with criminal punishments. In many cases, the victim's immediate need is not only to punish the offender, but also to quickly

¹³⁹ Hinduja and Patchin (n 2) 117–141.

¹⁴⁰ Convention on the Rights of the Child 1989, art 19.

¹⁴¹ Police Act 2020, s 4; Ihugba (n 10) 95–112.

¹⁴² *Solomon Okedara v Attorney-General of the Federation* (CA/L/174/18).

remove the content, get protective orders against further contact, stop further publication, and get help in stopping the harm that is already happening.¹⁴³ A victim-centered legal system should provide immediate injunctive and protective measures, rather than exclusively relying on eventual criminal trials.

Eighth, Nigeria should make it easier for privacy protection agencies and criminal law entities to work together. When cyberbullying includes doxxing, illegal sharing of personal information, or sharing private information that is too personal, the Nigeria Data Protection Commission should be more visible.¹⁴⁴ The police, prosecutors, and privacy regulators need to work together better so that the response makes more sense and works better.

Ninthly, public awareness and digital literacy must be treated as essential components of prevention. Cyberbullying is not a problem that law alone can solve. Schools, families, religious bodies, professional associations, civil society organisations and digital platforms should all participate in public education on responsible online conduct, empathy, privacy awareness and the legal consequences of cyber abuse.¹⁴⁵ Prevention is especially important because, once harmful material spreads online, complete restoration is often impossible.

Tenthly, digital platforms and service providers should be encouraged, and where lawful required, to maintain clearer community standards, user-reporting systems and content-response mechanisms relating to cyberbullying, especially where minors or intimate material are involved.¹⁴⁶ While private platform governance is not a substitute for law, it is an important line of first response in a digital environment where harmful material spreads rapidly.

143 Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s 24(4)–(6), as amended.

144 Nigeria Data Protection Act, 2023, ss 4–6.

145 Hinduja and Patchin (n 2) 141–160.

146 Citron (n 1) 177–203.

Eleventhly, Nigeria should encourage stronger inter-jurisdictional and international cooperation in relation to cyber offences. Cyberbullying often transcends geographical boundaries, and numerous offenders take advantage of this fact.¹⁴⁷ Mutual assistance, data-sharing protocols governed by law, and effective collaboration with platform operators and foreign entities would enhance the enforcement capabilities of the Nigerian legal system. Finally, the law should say that privacy can only be broken in a way that is legal, necessary, and fair. It is not right to treat anonymity and encrypted communication as perfect protections against abuse, but it is also not right to ignore them.¹⁴⁸ The proper approach is one of lawful balance: the privacy of users must be respected, yet credible cyberbullying complaints should be investigable under judicial and statutory safeguards.

5.3 Conclusion

It is an assault not only on emotion and reputation, but often on dignity, privacy, security and participation in public life. In Nigeria, the law has responded through constitutional guarantees, statutory provisions, evidential rules and institutional structures. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended, is the most important of these. It is backed by the Constitution, the Evidence Act, the Violence Against Persons (Prohibition) Act, the African Charter, and other legal documents.¹⁴⁹

The study has also shown that the current system is still not perfect. It is possible to prosecute serious online abuse under current law, but the system still has problems with vague definitions, inconsistent enforcement, technical issues, and the ongoing conflict between protecting victims

¹⁴⁷ Andrew Murray (n 22) 40–52.

¹⁴⁸ Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

¹⁴⁹ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015; Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024; Evidence Act, 2011; Evidence (Amendment) Act, 2023; Nigeria Data Protection Act, 2023; Violence Against Persons (Prohibition) Act, 2015.

and allowing free speech. A law against cyberbullying should not be used to shut down real criticism, but a democratic society should not let people who have been hurt by digital cruelty suffer in silence and despair.

The main point of this study is that Nigeria's legal system works, but it doesn't cover cyberbullying completely. Instead of getting rid of the current system, we need to make it better by making the laws clearer, protecting victims better, balancing the Constitution more carefully, improving digital investigations, raising awareness, and passing the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act of 2024, the Evidence Act of 2011, the Evidence (Amendment) Act of 2023, the Nigeria Data Protection Act of 2023, and the Violence Against Persons (Prohibition) Act of 2015. Only then can the law properly deal with cyberbullying while still upholding the constitutional values it is meant to protect.

`BIBLIOGRAPHY

Books

1. Aquinas T, Summa Theologica I-II, Q 90, Art 4
2. Austin J, The Province of Jurisprudence Determined (Prometheus Books 2000)
3. Babalola A, Law and Practice of Evidence in Nigeria (Sibon Books 2001)
4. Bernal P, Internet Privacy Rights: Rights to Protect Autonomy (Cambridge University Press 2014)
5. Citron D K, Hate Crimes in Cyberspace (Harvard University Press 2014)
6. Elias T O, The Nature of African Customary Law (Manchester University Press 1956)
7. Garner B A (ed), Black's Law Dictionary (11th edn, Thomson Reuters 2019)
8. Hart H L A, The Concept of Law (3rd edn, Oxford University Press 2012)
9. Hinduja S and Patchin J W, Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying (2nd edn, Corwin 2015)
10. Ihugba B U, Introduction to Legal Research Method and Legal Writing (Malthouse Press 2020)
11. Kenyon A T, Richardson M and others, Comparative Defamation and Privacy Law (Cambridge University Press 2016)
12. Ladan M T, Fake News, Cyber Bullying and Hate Speech on Social Media (Nigerian Institute of Advanced Legal Studies 2023)
13. Lloyd D, Introduction to Jurisprudence (6th edn, Sweet & Maxwell 1994)
14. Murray A, Information Technology Law: The Law and Society (4th edn, Oxford University Press 2019)
15. Nwadialo M N, Modern Nigerian Law of Evidence (University of Lagos Press 1999)

16. Ogbu O N, Human Rights Law and Practice in Nigeria (CIDJAP Press 2013)
17. Reed C and Angel J, Computer Law (7th edn, Oxford University Press 2019)
18. Reeves B and Nass C, The Media Equation: How People Treat Computers, Television and New Media Like Real People and Places (CSLI Publications 1996)
19. Simmonds N E, Central Issues in Jurisprudence (4th edn, Sweet & Maxwell 2018)
20. Wacks R, Privacy and Media Freedom (Oxford University Press 2013)
21. Weinreb L L, Natural Law and Justice (Harvard University Press 1987)

Journal Articles

1. Adediran A O, 'Cyberbullying in Nigeria: Examining the Adequacy of Legal Responses' (2020) International Journal for the Semiotics of Law 34(4) 965
2. Dodo D D, 'The Violence Against Persons (Prohibition) Act 2015: A Legislative Intervention against Gender-Based Violence in Nigeria' [2019] Ahmadu Bello University Law Journal 120
3. Eboibi F, 'A Critical Appraisal of Nigeria's Cybercrimes Act' [2017] University of Benin Law Journal 88
4. Eboibi F, 'A Critical Exposition of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act 2015' [2019] (5) DELSU Law Review 45
5. Ederagobor P, 'Section 24 of Nigeria's Cybercrime Act and its Impact on Freedom of Expression' (2025) SSRN Working Paper
6. Adeleke L and Oluwo Z A, 'The Legal Regime of Cyberbully and Victim Protection in Nigeria' [2025] Fountain University Law Journal 41
7. Kaplan A and Haenlein M, 'Users of the World, Unite! The Challenges and Opportunities of Social Media' [2010] (53) Business Horizons 59

8. McGlynn C, Rackley E and Houghton R, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' [2017] *Feminist Legal Studies* 25
9. Ojukwu S D and Agu O C, 'Legality of the Cybercrimes (Prohibition, Prevention, Etc.) Act as an Instrument for Internet Crimes Control in Nigeria' [2020] *Nnamdi Azikiwe University Journal of Commercial and Property Law* 7(2) 68

Newspaper and Online Sources

1. Channels Television, 'Court Sentences Lady to Three Years in Prison for Cyberstalking Eniola Badmus' (2 August 2023)
2. Premium Times, 'Court Grants Erisco Tomato Paste Reviewer Chioma Okoli N5 Million Bail' (31 May 2024)

Institutional Sources

1. Nigeria Computer Emergency Response Team (ngCERT), Official Mission Statement
2. Nigeria Police Force National Cybercrime Centre, Official Institutional Profile

