LEGAL CHALLENGES AND OPPORTUNITIES IN REGULATING DIGITAL CONTRACTS IN NIGERIA

BY

John Igenegbai NYAMALI

LAW2002896

FACULTY OF LAW
UNIVERSITY OF BENIN
BENIN CITY

NOVEMBER, 2025.

LEGAL CHALLENGES AND OPPORTUNITIES IN REGULATING DIGITAL CONTRACTS IN NIGERIA

BY

John Igenegbai NYAMALI

LAW2002896

A LONG ESSAY WRITTEN AND SUBMITTED TO THE FACULTY OF LAW, UNIVERSITY OF BENIN IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS (LL.B) OF THE UNIVERSITY OF BENIN, BENIN CITY.

NOVEMBER, 2025.

CERTIFICATION

I, **John Igenegbai NYAMALI**, with Matriculation Number **LAW2002896,** hereby certify that apart from references to other persons' works which have been duly acknowledged, the entire work is a product of my research, and this project has neither in whole nor in part, been presented for another degree elsewhere.

……..
John Igenegbai NYAMALI
LAW2002896

APPROVAL

We certify that this project was written and completed by **John Igenegbai NYAMALI**, with Matriculation Number **LAW2002896** in partial fulfilment of the requirements for the award of a Bachelor of Laws (LL. B) degree.

DR. (MRS.) S. AKINYELU ……..
PROJECT SUPERVISOR SIGNATURE AND DATE

DR. (MRS) O. F. OSUJI …….
PROJECT COORDINATOR SIGNATURE AND DATE

PROF. BRIGHT BAZUAYE ……
DEAN, FACULTY OF LAW SIGNATURE AND DATE

DEDICATION

This work is dedicated first of all to the Almighty God, the author of my life and also to my family for all their assistance to me.

ACKNOWLEDGEMENT

My gratitude goes to God, for protecting and sustaining me throughout the course of writing this project.

I am eternally grateful to my parents, Mr. and Mrs. Femi and Grace Nyamali, who have provided me with moral, emotional and financial support in my life. My heartfelt gratitude also goes to my siblings, Odufa, Eshemokhai, Danesi, Osilama and Omoiye, for their support and understanding. And to the rest of my family members who have supported me in one way or the other, I thank you all.

Endless appreciation goes to my Project Supervisor, Dr. Mrs. Akinyelu for her sense of direction, commitment and intellectual assistance she bestowed on me throughout the ordeal.

I am indebted to my friends, Onunu Alexander, Bello Jesse, Ogujor Rachael, Ehibor Success and Irabor Ivie, for their understanding and being with me through thick and thin.

Many thanks to wonderful friends like Festus-Iyaye Priye, Obakpolor Vestral, Ugberaese Peace, Yakubu Ojomon, Abu Leo and Omubo Fred for their support.

To my amiable class rep and assistant, Osamor Peace and Asirawede Kizito, and the entire Legal Luminaries Constituency, I express my profound gratitude to you all.

TABLE OF CONTENTS

TABLE OF CASES

TABLE OF STATUTES

Hire Purchase Act of 1965.

Marine Insurance Act, Cap. M2 LFN 2004, s. 24.

Hire-Purchase Act, Cap. H4 LFN 2004,

Arbitration and Conciliation Act, Cap. A18 LFN 2004,

Rotterdam Rules and the Nigerian Evidence Act, 2008

Constitution of the Federal Republic of Nigeria 1999

Federal Competition and Consumer Protection Act 2018

Cybercrime Act 2015

Nigerian Data Protection Act

Companies and Allied Matters Act (CAMA) 2020

Central Bank of Nigeria (Establishment) Act 2007

Banks and Other Financial Institutions Act 2020

Sale of Goods Act

Standards Organisation of Nigeria Act 1971

The Evidence Act 2011

Electronic Transaction Act (ETA)

Electronic Communications and Transactions Act No 25 of 2002

LIST OF ABBREVIATIONS

AC	Appeal Cases
ADR	Alternative Dispute Resolution.
AES	Advanced Electronic Signatures
All E.R	All England Report
AMA	Arbitration and Mediation Act
ATMs	Automated Teller Machines
BOFIA	Banking and Other Financial Institutions Act
C.A	Court of Appeal
CAMA	Companies and Allied Matters Act
CBN	Central Bank of Nigeria
ETA	Electronic Transaction Act
EU	European Union
FAA	Federal Arbitration Act
LCA	Lagos Court of Arbitration
LFN	Law of Federation of Nigeria
LMDC	Lagos Multi-Door Courthouse
LPELR	Law Pavilion Electronic Law Reports
NDPA	Nigerian Data Protection Act
NITDA	National Information Technology Development Agency

NWLR	Nigeria Weekly Law Reports
ODR	Online Dispute Resolution
QB	Queen's Bench
QES	Qualified Electronic Signatures
SON	Standards Organisation of Nigeria
UNCITRAL	United Nations Commission on International Trade Law
US	United States

ABSTRACT

The rapid expansion of digital technology has transformed traditional concepts of contract formation, execution, and enforcement. In Nigeria, digital contracts—ranging from online agreements and e-commerce transactions to fintech-based service contracts—have become increasingly common. However, despite their widespread use, the legal framework governing these electronic agreements remains fragmented and insufficiently developed. This thesis critically examines the legal challenges and emerging opportunities associated with regulating digital contracts in Nigeria. The study evaluates key statutes such as the Evidence Act 2011, the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, and the pending Electronic Transactions Bill, highlighting gaps in their capacity to address issues such as electronic signatures, admissibility of electronic evidence, jurisdictional complexities, automated contracting, and data protection. Using a doctrinal research methodology, the work draws on primary legislation, judicial decisions, scholarly writings, and comparative legal standards from jurisdictions such as the European Union and the United States. The findings reveal that while Nigerian law recognises electronic evidence and signatures to an extent, significant uncertainties persist in areas such as enforceability, consumer protection, and cross-border digital transactions. The absence of a comprehensive and consolidated statute on digital contracting continues to undermine legal certainty and trust in Nigeria's digital economy. Nevertheless, the study identifies opportunities for Nigeria to strengthen its regulatory landscape through legislative reform, harmonisation with international best practices, and institutional capacity-building. The thesis concludes that modernising Nigeria's digital contract framework is essential to promoting commercial growth, safeguarding consumer rights, and ensuring Nigeria's competitiveness in the global digital marketplace. It recommends the enactment of a robust Electronic Transactions Act, clearer judicial guidelines on electronic evidence, improved data protection mechanisms, and increased public awareness on digital rights and obligations. These reforms, if implemented, will enhance legal predictability and support Nigeria's transition toward a fully digitised commercial environment.

CHAPTER ONE

INTRODUCTION

1.1 Definition of Digital Contracts

The Black's Law Dictionary defines a Contract as, "A contract is an agreement between two or more parties that creates enforceable obligations or otherwise legally recognizable"[1]. From this definition of a contract, Digital Contract can also be defined as an electronic agreement between two or more parties, created and executed using electronic means without the need for paper or physical signatures. It functions as a digital version of traditional contracts, leveraging electronic data interchange and digital signatures to form legally binding agreements.

Digital contracts are legally binding agreements created, executed, and stored electronically. They encompass a wide range of formats—from simple email exchanges to complex smart contracts coded on blockchain platforms. These contracts are increasingly used in sectors such as e-commerce, fintech, telecommunications, and logistics, offering speed, automation, and reduced transaction costs.

Smart contracts, a subset of digital conztracts, are self-executing agreements with terms directly written into code. Once predefined conditions are met, these contracts automatically enforce obligations without human intervention. As noted by Omaplex Law Firm, smart contracts "do not rely on third parties or intermediaries for their execution and enforcement" and are "stored on a blockchain, written entirely in code".[2]

---

1 "Contract" definition, Black's Law Dictionary (12th Edition, June 2024)

2 Omaplex Law Firm, *Understanding Smart Contracts: Legal Implications, Benefits, and Challenges in Nigeria*, July 2025.

Despite their technological sophistication, digital contracts must still satisfy traditional legal elements—offer, acceptance, consideration, and intention to create legal relations—to be enforceable under Nigerian law.

1.2 Background to the Study

The digital transformation of commerce has led to the widespread adoption of digital contracts globally. In Nigeria, the rise of Information and Communication Technology (ICT) has facilitated digital transactions across various sectors. Contracts are now formed via emails, websites, mobile applications, and automated systems, often without physical interaction between parties.

However, Nigeria's legal framework has not kept pace with this evolution. The **Nigerian Evidence Act 2011** recognizes electronic records and signatures but lacks comprehensive provisions for digital contract formation. The **Cybercrimes Act 2015** addresses cyber fraud and data protection but does not regulate the nuances of digital contracting. The **Electronic Transactions Bill**, which aims to provide a robust legal framework, remains pending legislative enactment.

In contrast, jurisdictions like the **European Union** have adopted the **eIDAS Regulation**, which provides legal certainty for electronic identification and trust services. The **United States** enforces digital contracts under the **Electronic Signatures in Global and National Commerce Act (E-SIGN)**, ensuring that electronic signatures carry the same legal weight as handwritten ones.[3]

The absence of a consolidated legal regime in Nigeria creates uncertainty for businesses and consumers engaging in digital transactions. As digital contracts become the norm, Nigeria

---

[3] European Union, *eIDAS Regulation* (EU Regulation No 910/2014); United States, *Electronic Signatures in Global and National Commerce Act (E-SIGN)*, 2000.

must develop a legal framework that ensures enforceability, protects rights, and fosters innovation.

1.3 Statement of the Research Problem

Despite the increasing use of digital contracts in Nigeria, several legal uncertainties persist. There is a lack of comprehensive legal framework. There is no comprehensive and consolidated legal regime that directly addresses the peculiarities of digital contracts or unified statute that governs digital contracts in Nigeria. Existing laws are fragmented and do not address the peculiarities of electronic agreements, especially those formed through automated systems or blockchain platforms.

There is the problem of the admissibility of electronic evidence**.** While the Evidence Act recognizes electronic records, courts often struggle with interpreting electronic signatures and digital documents. The lack of judicial precedent on smart contracts further complicates enforcement.

Jurisdictional ambiguity is also a problem. Cross-border digital transactions raise complex questions about applicable law and forum for dispute resolution. Without clear jurisdictional rules, parties may face challenges in enforcing rights across borders.

Consent in automated agreements also hinders digital contracts. Automated contracts challenge traditional notions of consent. In smart contracts, parties may not explicitly negotiate terms, raising concerns about informed consent and contractual fairness.

Legislative delay in Nigeria. The delayed enactment of the Electronic Transactions Bill has left a legislative vacuum. This hinders business confidence and creates uncertainty for digital service providers and consumers.

These challenges underscore the need for legal reform to ensure that Nigeria's contract law reflects the realities of the digital age.[4]

1.4 Aim and Objectives of the Study

The main aim of this study is to critically examine the legal challenges and explore potential opportunities for regulating digital contracts in Nigeria. While the objectives include:

- To explore the nature and types of digital contracts used in Nigeria.
- To evaluate the adequacy of current Nigerian laws in regulating digital contracts.
- To identify legal challenges hindering enforceability and recognition.
- To propose legal and policy reforms for effective digital contract regulation in Nigeria.
- To draw comparative lessons from international legal frameworks on digital contracting

1.5 Scope and Limitations of the Study

This research focuses on the Nigerian legal framework governing digital contracts, with emphasis on both public and private sector transactions. It analyzes statutes such as the **Evidence Act**, **Cybercrimes Act**, and the **Electronic Transactions Bill**, alongside judicial decisions and academic commentary. The study also looks at the examination of digital contracts in sectors like fintech, e-commerce, and telecommunications, analysis of Nigerian statutes and pending legislation, and comparative review of international legal frameworks. The limitations of the study include the scarcity of data and the limited case law and judicial precedent on digital contract enforcement, legislative gaps and absence of enacted digital contract legislation constrains analysis, and technological fluidity along with rapid tech

[4] Grace Sunday-Ayegba, *Legal Enforceability and Jurisdictional Challenges of Smart Contracts in Nigeria*, Lawyard, September 2024.

evolution may outpace legal reforms. While global best practices are referenced, the study does not provide an exhaustive analysis of foreign laws.

1.6 Significance of the Study

This study is significant for several reasons which include legal development as digital contracts contribute to the discourse on modernizing Nigeria's contract law to accommodate digital realities. By identifying gaps and proposing reforms, the study supports the development of a coherent legal framework.

Policy reform is a significance as findings may inform legislative efforts to enact the Electronic Transactions Bill and related reforms. Policymakers can use the research to craft laws that promote digital innovation while safeguarding legal rights.

The study offers interpretive guidance for courts and judicial clarity in handling digital contract disputes. It highlights areas where judicial precedent is needed and suggests how traditional principles can be adapted.

Legal certainty in digital contracting can boost investor confidence and digital entrepreneurship. A robust legal framework will attract foreign investment and support Nigeria's digital economy ultimately leading to economic growth.

The research lays a foundation for further studies in digital law, cyber-jurisprudence, and legal tech giving it academic contribution. It encourages interdisciplinary exploration of law and technology in Nigeria.

As noted by Udo Udoma & Belo-Osagie, "the enforceability of smart contracts depends on traditional legal principles and their adaptation to new digital frontiers". Addressing these challenges is essential for Nigeria to thrive in the global digital economy.[5]

1.7 Research Methodology

The research will adopt a *doctrinal approach*, involving:

- Review of primary sources such as the Nigerian Constitution, Evidence Act, Cybercrimes Act, and judicial decisions.
- Examination of secondary sources including scholarly articles, law reports, and textbooks.
- Comparative legal analysis of international frameworks regulating digital contracts.
- Content analysis of government policy documents and proposed legislation such as the Electronic Transactions Bill. Where applicable, a case study approach will be used to highlight real-life examples of digital contract disputes and resolutions in Nigeria.

1.8 Structure of the Research

The research will be divided into five chapters:

- *Chapter One*: Introduction –definition, background, research problem, objectives, scope, and significance.
- *Chapter Two*: Formation of Digital Contracts – forming digital contracts, legal theories of contract formation, and technological contexts.

---

[5] Udo Udoma & Belo-Osagie, *Smart Contracts: Legal Implications in the Nigerian Capital Market*, August 2024.

- *Chapter Three*: Legal Framework and Challenges – analysis of Nigerian laws, challenges in regulation, and judicial treatment of digital contracts.
- *Chapter Four*: Comparative Analysis and Opportunities – study of legal systems such as the EU and the USA, and lessons for Nigeria.
- *Chapter Five*: Summary, Findings, and Recommendations – concluding insights and proposed legal reforms.

CHAPTER TWO

FORMATION OF DIGITAL CONTRACTS

2.2. Introduction

The law of contract remains one of the most fundamental aspects of private law, regulating the formation, validity, and enforcement of agreements between parties. In traditional contexts, contract formation followed a predictable pattern: offer, acceptance, consideration, capacity, and legality, executed physically through paper documents and manual signatures. However, the emergence of digital technology, particularly the internet, mobile applications, and blockchain, has transformed how contracts are formed. Today, agreements are increasingly concluded electronically, either through the simple click of an “I Agree” button, the provision of biometric data, or the automated execution of a blockchain “smart contract.”

The invention of electronic technology and the internet has changed the way we communicate, learn, work, and do business. It has brought the world’s people closer in time and space; businesses now work more efficiently with suppliers and consumers; consumers now have a greater choice and can shop from the comfort of their homes, offices, or even while travelling, for a wide variety of products, from sellers all over the world. Marketability of products is no longer confined to the boundaries of their nations. With a couple of clicks, one can buy and sell from any part of the world, and the desired product will be delivered at the buyer's doorstep. It is therefore not surprising that more businesses and consumers have developed an interest in this highly convenient and fast way of doing business. In this age of instantaneous and cross-border communications, electronic commerce (e-commerce) has truly become a global phenomenon.

In Nigeria, though e-commerce is still in its infancy, it is not left behind in this convenient way of doing business. This is evidenced by the rise and growth of e-commerce stores like Jumia, Konga, Dealdey, Gidimall, effritin.com, etc. and also the efforts by the government to enact a law that regulates electronic transactions[1]. However, a high percentage of businesses and consumers are still very wary about doing extensive business over the internet. This is primarily because of the risks associated with concluding a commercial transaction from a distance with an anonymous party (in most cases), the absence of a legal framework governing electronic transactions in Nigeria and the uncertainty surrounding the ability of parties to form valid and enforceable contracts via this paperless mode of communication. To facilitate e-commerce in Nigeria, these fundamental issues must be addressed.

The implications for legal theory and practice are profound. Nigeria, like many other jurisdictions, is confronted with the challenge of ensuring that contracts concluded electronically meet the requirements of enforceability under established legal principles. The difficulty lies not only in adapting existing doctrines of offer and acceptance to digital spaces but also in ensuring the authenticity of electronic signatures, the admissibility of electronic records, and the resolution of cross-border disputes. The novelty of electronic transactions makes it necessary to address some questions with respect to whether the traditional rules of contract formation can effectively be applied to the formation of electronic contracts; who makes the offer in click-wrap contracts, and when does acceptance become effective.

This chapter examines the formation of digital contracts in Nigeria. It begins by clarifying the concept of digital contracts and their various types, before considering how classical legal theories of contract formation apply in the digital environment. It then explores the technological frameworks that enable electronic contracting, the judicial treatment of such

---

[1] The Electronic Transactions Bill, 2011 which has been passed by the National Assembly, and is currently awaiting presidential assent.

agreements both in Nigeria and comparative jurisdictions, and the challenges that arise in their formation. The chapter concludes with reflections on the adequacy of the Nigerian legal framework and the need for reform.

2.3. Formation of Electronic Contracts

A contract is an agreement which gives rise to rights and obligations which can be enforced and recognised by law.[2] Under the common law, a contract is not required to take any particular form. It may be concluded expressly or by implication through a variety of methods, which include: correspondence through the post, telex or facsimile; orally, either in person or by telephone; or by completion of a formal document or a receipt,[3] provided the elements of a valid contract are present. Formation of electronic contracts, therefore, is not entirely different from formation of a contract via facsimile, post or telex; thus, a contract can be validly formed electronically provided all the elements of a valid contract are present.

Article 11 of the UNCITRAL Model Law on Electronic Commerce[4] provides that:

> In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.[5]

In most jurisdictions, the above provision might be seen as merely stating the obvious and therefore unnecessary. However, such provisions are very necessary in Nigeria, where recognition of the validity of electronic records is still viewed with suspicion and uncertainty.

---

2 E. Peel's Treitel*: The Law of Contract,* 12th edn. 2010.

3 Christensen S., "Formation of Contract by Email- Is it Just the Same as the Post", *QUTLJ,* [2001] (1) (1) 25.

4 Section 3 of the draft Electronic Transaction Bill 2011 has a similar provision.

5 For the purpose of the Model Law, 'Data message' means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.

The UNCITRAL Model Law on E-commerce does not make any specific provision as to when and where an offer and acceptance become effective. The reason given by the commission for this is that making express provisions as to the time and place an electronic contract is formed might interfere with the national law applicable to contract formation.[6] The writer thinks that the Model Law should have gone ahead to make express provisions as to when and where an electronic contract is formed, because this would aid in promoting harmonisation and dispelling the uncertainties surrounding the formation of contracts via electronic means. Besides, the Model Law serves as a guide to States that wish to enact or review their national laws on electronic commerce. Hence, the States reserve the right to disregard any provisions that interfere with their existing laws.

2.3.1. Offer and Invitation to Treat

It is pertinent to first analyse what constitutes an offer and invitation to treat in a traditional paper-based contract before delving into the issues in the formation of electronic contracts.

An offer is a promise made by one party to another with the intention that the promise will be legally binding on the offeror should it be accepted by the party to whom it is addressed. An offer becomes effective when it reaches the offeree. It must be definite and unambiguous.[7] It can be made to an individual, a group or the entire world.[8] However, where it is found that there is a lack of intention to be bound in a contract, then such a promise will be treated as an invitation to treat[9] rather than an offer. Acceptance of an offer creates a contract, while the acceptance of an invitation to treat is merely an offer.

---

6 Guide to enactment, Paragraph 78, UNCITRAL Model Law on Electronic Commerce.
7 *Oriental Bank Plc v. Bilante Intl*. [1997] 8 NWLR 515.
8 *Carlill v Carbolic Smokeball Coy* [1983] 1 QB 256.
9 This simply indicates a willingness to negotiate.

Electronic transactions are still an emerging area of law in Nigeria; therefore, there is currently no decided case as to whether a webvertisement constitutes an offer or an invitation to treat. This is important because an offer can be retracted at any time before acceptance. Once a party accepts the offer, the contract, in most cases, is concluded. Hence, disputes might arise as to the effectiveness of a revocation of the contract.

2.3.1.1. Offer - Website Trading

The display of goods with prices attached on a website can either be likened to the display of goods in a shop or an advertisement. The rules that apply to these two situations are somewhat different. Therefore, it is important to ascertain which party is the offeror and which party accepts the offer.

Where the goods displayed on a website are likened to the display of goods in a shop window or shelf, such a display constitutes an invitation to treat to which the buyer makes an offer by picking up the goods[10] and taking them to the sales clerk, who either rejects the offer or accepts the offer and receives payment for the goods.[11] The rationale for this rule is that the seller should not be bound to an unforeseeable number of acceptances. While the rationale may equally apply to the sale of goods via the internet, it might not apply to the provision of services or the sale of intangible products.[12] Nevertheless, if the display of goods, whether in a shop or on a website, was to be treated as an outright offer, then the seller would be bound to a contract as soon as a buyer accepts the offer by clicking or picking up the desired goods and taking them to checkout.

---

10 Or selecting the goods by a click of his mouse.

11 *Pharmaceutical Society of Great Britain v Boots Cash Chemists (Southern)* Ltd [1953] 1 QB 401, *Fisher v Bell* [1961] 1 QB 394

12 Software, music and information etc.

The rule governing advertisements is not as uncomplicated as that of a shop invitation. Some jurisdictions, for instance Brazil and Canada, consider an advertisement by a seller on a website as a binding offer, at least for a reasonable period of time, and when a prospective buyer places an order for goods on the website, such an order should constitute an acceptance. While in common law jurisdictions like the United Kingdom and Nigeria, the law views advertisements in two categories: those that pertain to bilateral contracts[13] and those that pertain to unilateral contracts.[14] In a bilateral contract, the advertisement is viewed as an invitation to treat, while the advertisement in a unilateral contract is viewed as an outright offer. In determining whether a webvertisement is a bilateral or unilateral contract, the words of the webvertisement and the objective intention behind it will be examined.[15] In instances where the website is non-interactive, the website displays the goods and gives information about the goods, the contract is then concluded through other means or face-to-face. Display of goods in this case will be viewed as an advertisement.

It will be to the advantage of the seller for the display of goods on the website to be likened to a shop display or viewed as a bilateral contract. In both cases, the seller reserves the option to accept or not to accept the order/offer of the buyer. This is so as to protect himself from being automatically bound to everyone who gets on the seller's website, regardless of their location. It also protects the seller in instances where there is a mistake in the statement of the price of goods or where the stock is depleted. The seller is, however, advised to make an express provision in the terms and conditions of sale that the display of goods on the website constitutes an invitation to treat and consequently an order by the buyer constitutes an offer which the seller can accept or reject.

---

[13] A bilateral contract takes the form of an exchange of promises. Whereas the offeror promises to do something in exchange of the offeree's promise to do something else in return. Although the contract has come into existence, there is yet to be performance.

[14] A unilateral contract takes the form of a promise in return for performance. The offeree has no obligation to perform the requested act neither does he need to communicate acceptance to the offeror.

[15] E. Todd's Gringras: *The Laws of the Internet*, 3rd edn. 2008 at pg. 25.

2.3.1.2. Offer – Electronic Mail (Email)

Contracts concluded via email are similar to the paper-based/traditional contracts, in that the parties usually negotiate the terms and conditions of sales by exchanging emails; therefore, it is easier to determine which party made the offer and which party accepted it by reading through the emails exchanged by the parties. In a case where the email received only displays the goods and their prices for the interested party to conclude the contract by other means, like telephone, fax or even face-to-face, then such a contract might likely be viewed as an advertisement. In such a case, the email from the seller could be construed as an offer[16] or an invitation to treat,[17] depending on the wording and the objective intention of the email.

2.3.2. Acceptance

Determining the time and place of an acceptance is of great importance in the formation of contracts. This is because the acceptance of an offer creates a legally binding contract. Besides, it determines the jurisdiction where the contract was formed. This is especially vital because e-commerce, by its nature, goes beyond boundaries; contracts can be entered into by parties in different jurisdictions.

For an acceptance to be valid, it has to be an absolute and unqualified expression of assent to the terms of the offer.[18] It may be manifested by words or conduct.[19] However, silence or inactivity does not amount to acceptance.

Where the offeror prescribes a mode by which acceptance may be communicated in mandatory terms, the prescribed mode must be followed; else the acceptance is invalid. Where the offeror does not insist that only acceptance in the prescribed mode shall be binding,

---

16 *Carlill v Carbolic Smokeball Coy* [1983] 1 QB 256
17 *Granger & Son v Gough* [1896] AC 325
18 I. E. Sagay's *Nigerian Law of Contract,* 2nd edn. 1999 pg 20
19 *Orient bank (Nig.) Plc v Bilante International Ltd* [1997] 8 NWLR (Pt 515)

then any other mode which is faster than or at least equally as fast as the prescribed mode may be used.[20] Where no method of acceptance is prescribed, the general rule is that acceptance may be given by the same or by a method equally as fast as the method used in making the offer.

In traditional contract law, acceptance becomes effective not merely when communicated, but when actually received by the offeror.[21] Until an acceptance is received by the offeror, the offer may be revoked. The main rationale for this rule is that it could cause hardship to the offeror if he is to be bound without knowing that his offer has been accepted. However, the 'postal acceptance rule' is an exception to this general rule.

The postal acceptance rule states that, where acceptance is to be communicated to the offeror via the postal system, then acceptance becomes effective when posted[31], rather than when it reaches the offeror.[22] Consequently, the contract is made once posted and therefore may not be revoked. The rationale for this rule is that the post office is treated as a common agent of both parties[23]and that it is easier to prove that a letter has been posted than that it has been received,[24] but this cannot be a justifiable reason in this modern times where the sender of a mail could request that the receiver acknowledges receipt. Another reason given is business convenience, without the rule no contract will ever be completed by the post, because if the offeror was to be bound only when he has received the acceptance then the offeree should not also be bound until he receives a confirmation from the offeror that his acceptance has been received and accented to it, it might go on *ad infinitum*. The postal acceptance rule was

---

[20] *Manchester Diocesan Council of Education v Commercial and General Investments Ltd* [1969] 3 All E.R. 1593

[21] *Entores v Miles Far East Corporation* [1955] 2 Q.B. 327 C.A*, Anon Lodge Ltd v Merchantile Bank* [1993] 3 NWLR (Pt 284) 721 31. *A letter is deemed posted when it is out of the control of the acceptor and in the control of the post office or of one of its employees who is authorized to receive letters.*

[22] *Adams v Lindsell* [1818] 1 B

[23] *Dunlop v Higgins* 1 H.L.C 381

[24] Treitel*: The Law of Contract*, 12 edn. 2010

developed at a time when postal system was the only means of communication between distant parties.[25] With the emergence of faster and more reliable means of communication[26] one cannot help but wonder if this rule should still be applied in modern times. There is presently an ongoing debate as to the fairness of this rule, however, it is beyond the scope of this article to join this active debate.

The postal acceptance rule also applies to telegrams and courier services but not to forms of communication that are taken to be instantaneous, for instance telephone, faxes and telexes. In the case of *Entores Ltd v Miles Far East Corporation*,[27]Denning L.J stated that in instantaneous communications, the acceptor will often know that his attempt to communicate was unsuccessful, and is under the duty to ensure that the communication is properly made.[28]

However, it remains unclear which of the rules of acceptance will be applied to electronic communication of acceptance. Will it be the 'receipt rule' of acceptances where electronic communications will be treated as instantaneous or the 'postal acceptance rule'?

2.3.2.1. Acceptance via Electronic Mail (Email)

It has been argued that email communications should not be categorised as instantaneous communication, because just like the postal system, there is no direct connection between the sender and the recipient. It involves the participation of third-party Internet Service Providers (ISPs), whose servers receive and send emails via mailboxes.[39] ISP acts like the post office. This third-party involvement makes email communications potentially subject to third-party delays, which could be caused by technical issues. Thus, there is no certainty as to when an email communication may be received. Given that the mail is put beyond the control of the

---

[25] *Scottish Law Commission, "Review of Contract Law, Discussion Paper on Formation of Contract"* 2012 pg. 58

[26] *Telex and Facsimile*

[27] (1955) All E.R. 493

[28] E. Peel's Treitel*: The Law of Contract,* 12th edn. 2010

sender once transmitted, he should not be made liable for any faults which may occur after transmission. Also, the contracting parties themselves may also contribute to the delay by addressing the mail wrongly, or even reading the delivered mail late.

However, the postal acceptance rule should not be applied to email communications merely because it shares some similarities with the postal system. Most other instantaneous communications also rely on the participation of third parties, for instance, the telephone, telex, etc., where there are also third-party involvements like the telecommunication network providers, who might also cause some delays in communication. Secondly, the postal acceptance rule was developed at a time when the postal system was the only means of distance communication. However, today, there are faster and more effective means of distance communication, so the rationale that the postal acceptance rule avoids the continuous exchange of mail *ad infinitum* does not apply to electronic communications. Also, there are software's that can inform the sender when his email has been delivered and read. Most often, the sender will be notified when delivery of an email has failed, but the receiver, on the other hand, has no way of knowing that there has been a failed attempt at sending him an email accepting his offer. The sender's knowledge of the status of the email in transmission and duty to ensure the offeror receives the acceptance should be the yardstick for determining where to categorise electronic communication. Finally, with the availability of other forms of instantaneous communication, the parties involved can ensure that there is no extended lapse in communication.

Due to the hardship and injustice that the application of the postal acceptance rule has caused, most countries are already working on the reform of their contract law in order to limit the application of the rule. Additionally, courts seem reluctant to extend the application of the

postal acceptance rule to other modes of communication, such as fax, unless it is perceived that the parties contemplated the use of the rule in their contract.

Whether the court chooses to apply the 'receipt rule' or the 'postal rule,' there remains the question of when an electronic communication is deemed to be dispatched and received. Article 12,[29] of the UNCITRAL Model Law on Electronic Commerce clarifies when and where a message is deemed to have been dispatched and received. It states that an electronic communication is dispatched when it enters the information system outside the control of the sender and received when it enters the designated information system of the receiver or when accessed. Section 19 of the Electronic Transactions Bill further provides that where the sender and the receiver use the same information system, then electronic communication is deemed to be sent when it is capable of being received and processed by the receiver.

2.3.2.2. Click-wrap Acceptance

Unlike acceptance communicated via email, a click-wrap acceptance in a website trade is less complicated. It has been described as having the same quality as telephone communication,

---

[29] Article 12 (1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or the person who sent the data message on behalf of the originator.
(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:
(a) If the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:
(i) At the time when the data message enters the designated information system, or
(ii) If the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee.
(b) If the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.
(2) Paragraph (2) applies notwithstanding that the place where the information system may be different from the place where the data message is deemed to be received under paragraph (4).
(3) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For this paragraph:
(a) If the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction, the principal place of business.
(b) If the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

but between computers rather than humans.[30] The communication is usually interactive and automated. The software controlling the transactions allows contracting parties to determine whether an agreement has been reached or not. Acceptance via an interactive e-commerce website can safely be categorised as an instantaneous communication, and the 'receipt rule' of acceptance will therefore be applied.

2.3.3. Consideration

For a contract to be valid, there must be consideration, among other elements of a valid contract[31]. Consideration can be described as a promise by a party to another, to do something in return for the promise of the other party. Each party must obtain a benefit from the contract. In the case of e-commerce, this is rarely an issue because, like the paper-based commercial transaction, the buyer usually receives the goods while the seller receives payment.[32]

2.4. Authentication of Electronic Contracts

There are various reasons why some parties might prefer the traditional paper-based mode of contracting to the electronic mode; one of the main reasons is the ability of the parties to endorse the contract.

In paper-based contracts, signatures are generally used to identify the parties to a contract; to provide certainty as to the personal involvement of the party in the act of signing and to attest to the intent of the party to endorse authorship of the document written by himself or on his behalf; and to associate that party with the content of the document. [33]Authentication could take the form of a handwritten signature, thumbprint, stamping, or even a typewritten signature. However, these authentications are usually linked to paper-based contracts.

---

30 E. Todd's Gringras*: The Laws of the Internet,* 3rd edn. 2008 at pg. 41
31 Ibid.
32 Ibid.
33 UNCITRAL model guidance note.

Apart from most parties' desire to have their contracts authenticated as an assurance of genuineness, there are instances where the law might require that an agreement be signed if it is to be deemed as valid and enforceable.[34]

There are now technologies that allow for the authentication of an electronic document. With the availability of scanners and PDF documents, identification documents can be made available electronically.

On the question of the legality of electronic signatures,[35] section 93 of the Evidence Act 2011 provides that electronic signatures are admissible. This issue has also been addressed in the UK by the enactment of the Electronic Signatures Regulation 2002 and the Electronic Communication Act 2000, which promotes the use of digital signatures and provides that electronic documents should not be denied enforceability merely on the grounds that it is in electronic form.

The UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures[36] deal with electronic communications and signatures in the context of commercial activities. The Model Laws provide that electronic signatures shall have legal effect once they satisfy the criteria. The Model Law on Electronic Commerce adopted the 'functional equivalent approach in dealing with electronic signature and other formal requirements. This means that it identifies the basic function of the legal form requirement, provides criteria which, once met by the electronic record, enable the record to enjoy the same level of legal recognition as the corresponding paper-based documents performing the same function. In the case of 'signature,' it identified its function in a paper-based

---

34 For instance, a hire purchase agreement under the Hire Purchase Act of 1965.

35 Article 2 (a) of the UNCITRAL Model Law on Electronic Signature defines electronic signature as '…data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message, and to indicate the signatories approval of the information contained in the data message'.

36 Adopted in 2001

environment as including: identification of parties; provision of certainty as to the personal involvement of that person in the act of signing; and the association of the person with the content of the document.[37] The law then provides that an electronic signature must have the ability to identify the person and indicate the approval of that person of the content of the message, and that it must be sufficiently reliable in all circumstances. The Model Law, however, does not provide any guidance as to how the electronic signature may be created to meet the requirements.

Electronic signatures, just like paper-based signatures, do not have to be generated in any particular form.[38] It could be created by simply typing one's name and initials, making any mark in the designated area through the use of encryption software or through a connected fingerprint device, etc. The courts also retain the discretion to question the reliability and authenticity of a handwritten signature as well as an electronic signature.

2.5. Judicial Treatment of Digital Contracts in Nigeria

Although digital contracts are increasingly common, Nigerian courts have only gradually begun to engage with disputes arising from them. Judicial pronouncements are critical because statutory provisions alone cannot capture the dynamism of electronic commerce. Courts must interpret these statutes and apply established contract doctrines to novel contexts.

In *Stanbic IBTC Bank v Longterm Global Capital Ltd*[39], the Court of Appeal in this case upheld the admissibility of electronically generated bank statements as evidence of contractual obligations. The decision affirmed that section 84 of the Evidence Act 2011 applies to digital contracts, provided proper certification is presented. This case illustrates the judiciary's recognition of electronic records as binding evidence in commercial disputes.

---

37 Guide to Enactment 1996, Paragraph 48

38 E. Todd's Gringras*: The Laws of the Internet,* 3rd edn. 2008 at pg. 25

39 (2018) LPELR-CA/L/1095/2016.

2.6. Challenges Associated With Online Contracts

a. Contracts which must be in Writing: The Statute of Frauds

While the general rule is that contracts may be made in writing, orally or even by conduct, there are species of contracts which are required to be evidenced in writing. Often, there is a need to execute these contracts accordingly, by signing or making a mark. Thus, contracts for hire-purchase,[40] agreements between master and seamen,[41] marine insurance policies,[42] bills of sales, bills of exchange,[43] money-lender's contracts, legal practitioner's agreement with his client for remuneration, pawn-broker's agreement for a pledge, arbitration agreements,[44] declaration of trusts respecting land and dispositions of interests in land[45] must be made in writing and executed accordingly. The Statute of Frauds, in some cases, requires contracts to be evidenced in writing. In order to vary such contracts, further writing is also required. Since the essence of the Statute of Frauds is that the contract should be reduced in tangible form, internet contracts obviously satisfy this requirement. It is therefore necessary that electronic communications, such as emails, be preserved in printed form or a computer log.[46]

A problem is likely to arise with contracts which are required not just to be in writing but to be signed or embodied in a deed, or even those required to be authenticated by a notary public or a magistrate – illiterate jurat. This is because for contracts formed online, the traditional form of paper and handwritten signatures does not exist, to say the least, of thumbprints. The issue, then, is how online contracts could meet this requirement. Email

---

40 Hire-Purchase Act, Cap. H4 LFN 2004, s. 2(1) & (2).

41 Seamen's Articles of Agreement Convention 1926 (No. 22), Art. 3.

42 Marine Insurance Act, Cap. M2 LFN 2004, s. 24.

43 Bills of Exchange Act 1882, s. 3.

44 Arbitration and Conciliation Act, Cap. A18 LFN 2004, s. 1.

45 Statute of Frauds 1677, s. 4.

46 John S. Foster, "Electronic Contracts and Digital Signatures," available at http://www.corbinball.com/articles_legal/index.cfm?fuseaction=cor_av&artID> accessed 29th September 2025. see also Victor Chandler International v. Customs &Excise Commissioners [2000] 1 WLR 1296 where it was held that electronically stored information can in law constitute a document.

exchanges will satisfy the requirement of the Statute of Frauds where an intention to authenticate the communication is evinced.[47] To determine an intention to authenticate the communication, the court will usually consider what manner of email account was used – i.e. whether it is a business or personal email account, (a vital point in this regard would involve an enquiry as to the purpose assigned to the various email accounts by the sender); use of real names or aliases and where the alias is used, knowledge of the recipient of the alias; analysis of the content of the communication to discover the intention of the sender to authenticate it; prior dealings between the parties and usual practices in the business which is the subject of the email contract.[48] There is a strong indication that the sender intends to authenticate the communication, where he indicates his name at the bottom of the email, the usual space for a signature.[49]

The requirement of a signature can be satisfied in the case of electronic documents by a digital signature, by typing a name into an electronic document or even by clicking on a website button. This is buttressed by Section 93(2) of the Evidence Act 2011, which reads: "Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences."

Section 93(3) goes further:

> All electronic signatures may be proved in any manner, including by showing that a procedure existed by which a person must proceed further with a transaction to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

---

47 Ibid.

48 Ibid.

49 *Rosenfeld v. Zernec,* 776 N.Y. Sup. 2004).

In *Joseph DeNunzio Fruit Co. v. Crane*[50] a federal court in Los Angeles held that an exchange of teletype messages satisfied the California Statute of Frauds, which at that time provided that a contract for the sale of goods or choses in action valued at $500 or more "shall not be enforceable by action unless... some note or memorandum in writing of the contract, or sale be signed by the party to be charged, or his agent in that behalf." The court acknowledged that the teletype messages did not bear the signature in writing of the party to be charged "in the sense that they were not literally signed with pen and ink in the ordinary signature of the sender."[51] Nevertheless, the court considered that:

i. Each of the parties had teletype machines in their respective offices that "would type the message or memorandum simultaneously in the other office...."
ii. Each party was readily identifiable and known to the other by the symbols or code letters used.
iii. There was no contention that the messages did not originate in the office of the other.

Consequently, the court, per Judge O'Connor, stated that the courts:

> Must take a realistic view of modern business practices, and can probably take judicial notice of the extensive use to which the teletype machine is being put today among business firms, particularly brokers, in the expeditious transmission of typewritten messages.[52]

In *Hillstrom v. Gosnay,*[53] the Montana Supreme Court held that the typewritten name: "JEREMI VILLANO M" at the bottom of a telegram satisfied the requirements of the Montana Statute of Frauds and also satisfied the requirement for authentication by signature. The court emphasised that the requirement for a written memorandum "may consist of any type of writing." Again, in *Hessenthaler v. Farzin,*[54] a Pennsylvania court held that a mailgram confirming acceptance of a real estate offer satisfied the Statute of Frauds

---

50 79 F. Supp. 117 (S.D. Cal. 1948); 342 U.S. 820 (1951).
51 79 F. Supp. 117 at 128.
52 Ibid, at pp. 128- 129.
53 188 Mont. 388, 614 P.2d 466 (1980).
54 388 Pa. Super.37, 564 A.2d 990 (Pa. 1989).

requirement for contracts for the sale of land to be signed and in writing. A key consideration upon which the court based its judgment was "whether there is some reliable indication that the person to be charged with performing under the writing intended to authenticate it."[55] The court stated that "the proper, realistic approach in these cases is to look at the reliability of the memorandum, rather than to insist on a formal signature."[56] Analyzing the mailgram to confirm its compatibility with the intent of the Statute of Frauds, the court found that:

> The detail contained in this mailgram is such that there can be little question of its reliability. Appellants were careful to begin the mailgram by identifying themselves. They then made certain that their intention would be properly understood by declaring their acceptance and identifying both the property and the consideration involved. In light of the primary declaration of identity, combined with the inclusion of the precise terms of the agreement, we are satisfied that the mailgram sufficiently reveals appellant's intention to adopt the writing as their own, and thus is sufficient to constitute a "signed" writing for purposes of the Statute.[57]

The above decision has been approved and followed in *Flight Systems, Inc. v. Electronic Data Systems Corp.,*[58] where it was held that a typewritten name on the stationery of the defendant's legal affairs department, which was initialled by the sender and transmitted by facsimile, met the requirements of the Statute of Frauds when considered in conjunction with other documents. The court stated that "any mark or symbol – including a typewritten name – will be deemed to constitute a signature for the Statute if it is used with the declared or apparent intent to authenticate the memorandum."[59]

---

55 Ibid., at p. 42.

56 Ibid., at pp. 43-44.

57 Ibid, at p. 44.

58 112 F. 3d 124 (3d Cir. 1997).

59 In the United States a federal statute: the Electronic Signatures in Global and National Commerce Act 2000 (ESIGN) and the Uniform Electronics Transactions Act (UETA) adopted by majority of the States provide that "if a law requires a record to be in writing, an electronic record satisfies the law", and also that "if a law requires a signature, an electronic signature satisfies the law" – ESIGN s. 101(d); UETA s. 7. See also P. Quick and J. A. Rothchild, "Consumer Protection and the Internet," in Handbook of Research on International Consumer Law, G. Howells et al eds. (UK: Edward Elgar Publishing Ltd., 2010), p. 344.

Contrastingly, in *Parma Tile Mosaic & Marble Co. v. Estate of Short,*[60] the New York Court of Appeals held that the automatic printing by a fax machine of a sender's name at the top of each page transmitted was insufficient to satisfy the requirement of the Statute of Frauds. The Court held that the act of identifying and sending a document to a particular destination did not, by itself, constitute a signing authenticating the contents of the communication.[61]

b. Developing an Effective Legal Framework for Online Contracts

In order to effectively address the challenges posed by online transactions, Nigeria must put in place robust, effective and enforceable legal instruments that will drive the new trend of online transactions. The Nigerian legal system is disappointingly backward and empty in this regard. Bill 53, which seeks to provide for legal recognition of commercial transactions through the use of electronic means, which is currently before the National Assembly, is a step in the right direction. It is hoped that it will soon be passed and not, as one writer puts it, "suffer the same fate as the Electronic Messages, Information and Commerce and its Admissibility in Evidence and Related Matters Bill 2004, which was never passed into law."[62] Also, Nigeria does not have any law for cybercrime. What is close to this is the Advanced Fee Fraud and Other Fraud Related Offences Act 2006, which, in Part II, provides for Electronic Telecommunication Offences. It mandates the telecommunication providers to maintain a database of all their subscribers and to make same available to the Economic and Financial Crimes Commission on demand. It, thus, falls short of the expectations of combating modern cybercrimes.[63]

---

60 87 N.Y. 2d 524, 663 N.E. 2d 633 (N. Y. 1996).

61 *Cf. Bradley v. Dean Witter Realty Inc*. 967 F. Supp. 19 (D. Mass. 1997) and *Birenbaum v. Option Care, Inc.* 971 S. W. 2d 497 (Tex. App. 1997). Electronic Commerce (Provision of Legal Recognition) Bill 2011.

62 H. A. C. Umezuruike, "Electronic Bills of Lading, Rotterdam Rules and the Nigerian Evidence Act," *The Nigerian Law Journa*l, Vol. 16 No. 1 (2013), p. 71.

63 See M. M. Akanbi et al, "An Appraisal of the Nigerian Advance Fee Fraud and Other Fraud Related Offences Act 2006," *The Nigerian Law Journal,* Vol. 16 No. 1 (2013), p. 126.

Happily, the international community is replete with legislation on online transactions and for fighting cybercrimes, which can aid Nigeria in drafting appropriate laws for the same purpose. Prominent is the United Nations Convention on the Use of Electronic Communications in International Contracts (ECC).[64] Prior to this Convention, there were the UNCITRAL Model Law on Electronic Commerce (MLEC) 1996 and the UNCITRAL Model Law on Electronic Signatures (MLES) 2001. These last two are not treaties but model laws that set out standard legislative texts for e-commerce. The ECC then updated and complemented these model laws in order to increase uniformity and predictability in international trade law. It achieved this by adopting the fundamental principles of the uniform law of electronic commerce entrenched by UNCITRAL, which are non-discrimination, technological neutrality, functional equivalence and irrelevance of place of origin.[65]

The benefits of the UNCITRAL rules are evident in their provisions, such as that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form or that a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation. Again, in the area of international carriage of goods, another contribution of UNCITRAL is the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea 2008, which provides for the use of electronic transport records as an alternative to paper documents if the carrier and the shipper agree on this. The UNCITRAL Model Laws are meant to provide guidance to

---

64 This was prepared by the United Nations Commission on International Trade. Law (UNCITRAL) and adopted by the UN General Assembly on 23 November 2005. Also called the Electronic Communications Convention (ECC), it is a treaty that aims at facilitating the use of electronic communications in international trade. See <http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf> accessed 29th September 2025. As at November 2013, the Convention has been signed by 18 States and ratified by three States: Dominican Republic, Honduras and Singapore which are State Parties to the Convention and it came into force for these States on 1 March 2013. Nigeria is neither a signatory nor a party to the Convention. See <http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=X18&chapter=10&lang=en> accessed 29th September 2025 for a list of signatories.

65 L. Castellani, "The United Nations Electronic Communications Convention – Policy Goals and Potential Benefits," 19(1) *Korean Journal of International Trade and Business Law*, Vol. 1 (2010), p. 2.

municipal legislation, and the Convention is aimed at ensuring some uniformity in international e-commerce trade.

It is worthy of mention here, as a way of comparison, that Singapore ranks among the first developing countries to promulgate a law on electronic transactions. The Electronic Transactions Act (ETA) 1998 is an adaptation of the ECC and the UNCITRAL Model Laws on Electronic Commerce and Electronic Signature.[66] Specifically, burning issues on electronic transactions such as commercial code for e-commerce, electronic applications for the public sector, liability of network providers, security procedures for public key infrastructures and biometrics were addressed in this legislation. It is urged that Nigeria should borrow a leaf from Singapore in order to meet the challenges of the ever-changing ICT world. Many other countries of the world[67] have also passed legislation along the lines of the model laws and the Convention, so that some uniformity in the law of e-commerce is in sight, and it is hoped that Nigeria will follow suit.

c. Infrastructural Challenges

A major challenge to contracting online in Nigeria is infrastructural inadequacy. At the height of this lack is electricity. Without power, the electronic gadgets cannot work. Where transactions are contracted through emails, for instance, it is possible that one of the contracting parties may not even be able to read their mail, in order to respond appropriately for lack of electricity.

---

66 Interestingly, Singapore has amended their ETA five times since 1998 in order to keep abreast with the rapid developments in ICT. The last amendment was in January 2013. See http://statutes.agc.gov.sg/aol/home.w3p. > accessed 30th September 2025.

67 See for example the UK Consumer Protection (Distance Selling) Regulations 2000 which implemented the 1997 EU Directive on the protection of consumers in respect of distance contracts; Egypt's E-signature and Establishment of the Information Technology Industry Development Authority Law No. 15 of 2004; Ghana's Electronic Transaction Act 2008; Kenya's Communications (Amendment) Act 2008; Tunisia's Electronic Exchanges and Electronic Commerce Law 2000 and Uganda's Electronic Transactions Act and Electronic Signature Act, both of which were passed in 2011 – see N. Ewelukwa, "Is Africa Ready for Electronic Commerce? A Critical Appraisal of the Legal Framework for Ecommerce in Africa" available at http://www.acicol.com/__temp/Dr_N.pdf accessed 20th September 2025.

Another major challenge in online contractual transactions in Nigeria is poor internet service. Internet access is hardly available, and when available, it is very slow, erratic and epileptic. There is also very low internet penetration. As a result, people rarely place reliance on internet services, which are the fulcrum upon which online business gravitates. It is common knowledge that whole banking businesses are shut down for hours on end, or worse, even for days, on the usual excuse that the server is down.

Common automated registrations via filling out online forms are often unreliable as a result of poor internet service. For unknown reasons, government and other corporate organisations in Nigeria are notorious for a lack of consistency in maintaining their websites. It is doubtful that meaningful contractual relations could result or be encouraged under such situations.

2.7. Conclusion

The formation of digital contracts in Nigeria is firmly rooted in traditional contractual principles but complicated by the peculiarities of electronic communication and technology. Statutory provisions such as sections 84 and 93(2) of the Evidence Act 2011, the Cybercrimes Act 2015, and CBN regulations provide partial recognition of electronic contracts, while judicial decisions demonstrate the courts' willingness to address disputes in this area. Nevertheless, challenges persist, including difficulties in establishing informed consent, verifying capacity, addressing cross-border conflicts of law, and ensuring adequate consumer protection. Nigeria must therefore strengthen its legal framework, particularly through the passage of the long-delayed Electronic Transactions Bill, and align with international best practices such as the UNCITRAL Model Law and the EU Directive on E-Commerce. Only then can the formation of digital contracts in Nigeria achieve the certainty, security, and enforceability necessary to support the nation's growing digital economy.

CHAPTER THREE

LEGAL FRAMEWORK AND CHALLENGES IN REGULATING DIGITAL CONTRACTS IN NIGERIA

3.1. Introduction

Contracts have always formed the backbone of commercial transactions, providing certainty and enforceability in exchanges of goods, services, and obligations. In Nigeria, like in most common law jurisdictions, contract law is traditionally rooted in English common law principles such as consensus ad idem, offer and acceptance, consideration, intention to create legal relations, and capacity. However, the rise of digital technology has disrupted the conventional contract landscape. Increasingly, contracts are formed, executed, and performed electronically through emails, websites, mobile applications, blockchain platforms, and other digital interfaces. This digital shift has created both opportunities and challenges. On one hand, digital contracts reduce transactional costs, allow instantaneous cross-border dealings, and expand commercial opportunities for Nigerian businesses in global markets. On the other hand, the peculiarities of electronic transactions questions of authenticity, jurisdiction, applicable law, consumer protection, cybersecurity, and enforceability raise legal issues that the traditional framework was not originally designed to address. This chapter explores the Nigerian legal framework regulating digital contracts, statutory developments, judicial treatment, and the challenges arising in practice.

3.2. Nigerian Legal And Regulatory Framework

Nigeria has firmly established itself as a player in the global e-commerce and digital trade arena, reaping significant benefits from this trend. This growth has spurred development in various industries, driven largely by the internet and the innovation of investors and tech

entrepreneurs.[1] However, the lack of comprehensive legal regulations has left many aspects of this industry vulnerable. Effective regulation of e-commerce in Nigeria is essential for the country's commercial and economic advancement. It creates a framework that guides industry participants and assures consumers that services comply with established standards. Moreover, such regulations enable the government to generate revenue, which can be reinvested into the economy. As Nigeria works to strengthen its legal framework for this sector, it is important to examine existing laws and their implications for fostering a secure and thriving digital marketplace.

3.2.1. Constitution of the Federal Republic of Nigeria 1999

The Constitution of the Federal Republic of Nigeria 1999 stands as the supreme law of the land[2], providing a vital legal and governance framework essential for the nation's operations. It delineates the structure of government, encompassing the three branches and defining the relationship between the state and its citizens. Central to this framework is the articulation of fundamental human rights, legislative and executive powers, and judicial authority, which collectively establish the legal boundaries within which laws concerning e-commerce and digital trade are developed.

While the Constitution does not explicitly address e-commerce or digital trade, its provisions can be interpreted to encompass these domains. As the grundnorm of Nigeria, the Constitution's supremacy over all other laws is affirmed in Section 1(3),[3] ensuring that any legislative measures related to e-commerce must align with its principles. Furthermore,

---

1 Akinpelu A.O., Legal Issues in Regulating the E-commerce Sub-Sector in Nigeria, <https://www.scribd.com/document/333534315/Legal-Issues-in-Regulating-the-E-commerce-Sub-sector-in-Nigeria> accessed 29th September 2025.

2 Section 1, Constitution of the Federal Republic of Nigeria 1999 (as amended).

3 Constitution of the Federal Republic of Nigeria 1999.

Section 4 empowers lawmakers to create laws, thereby facilitating the enactment of regulations governing digital transactions.

A key provision relevant to e-commerce is found in Section 37, which guarantees the privacy of citizens, encompassing their homes, correspondence, telephone conversations, and telegraphic communications. This clause can be construed to protect online transactions and the privacy of users engaged in e-commerce activities. In addition, the Constitution supports fundamental rights such as freedom of expression,[4] which safeguards consumers' right to voice their opinions, and the right to a fair hearing, ensuring consumers are treated justly in legal matters.[5] The dignity of individuals is also protected, which, in turn, affirms the respect that must be afforded to consumers.[6]

Undoubtedly, the Constitution provides a foundational legal basis for the principles influencing the e-commerce and digital trade landscape. Its provisions not only advocate for consumer rights and protections but also lend legal recognition to electronic transactions, thereby fostering an environment conducive to digital commerce. Understanding this constitutional framework is crucial for comprehending the broader legal dynamics surrounding e-commerce in Nigeria.

3.2.2. Federal Competition and Consumer Protection Act 2018

The Federal Competition and Consumer Protection Act (FCCPA), enacted in 2018, represents a significant legislative advancement in the Nigerian regulatory landscape, particularly concerning e-commerce and digital trade. Its establishment led to the formation of the Federal Competition and Consumer Protection Commission, a pivotal agency operating under the Federal Ministry of Trade and Investment. The Commission is tasked with

4 Section 39, Constitution of the Federal Republic of Nigeria 1999
5 Section 36, Constitution of the Federal Republic of Nigeria 1999
6 Section 34, Constitution of the Federal Republic of Nigeria 1999.

fostering fair, efficient, and competitive markets within the Nigerian economy, ensuring that all citizens have access to safe products and that their rights as consumers are well-protected.[7]

The primary objectives of the FCCPA extend beyond mere consumer protection; they are designed to drive fair competition and safeguard consumer interests in an increasingly digital marketplace. By regulating practices that could potentially mislead consumers, the FCCPA creates a framework for transparent commercial interactions. Section 73 of the Act[8] explicitly states: "A business shall not engage in any unfair practice that may deceive or mislead consumers." This provision serves as a fundamental pillar for establishing trust between businesses and consumers in an era where e-commerce transactions are growing immensely.[9]

One of the core aims of the FCCPA is to foster and sustain competitive markets by prohibiting restrictive agreements and preventing the abuse of dominant market positions. This aspect is particularly crucial for e-commerce platforms that often dominate the digital marketplace. The law seeks to ensure that no single business can manipulate market conditions to the detriment of competitors and consumers alike, thereby ensuring a level playing field for all market participants.

In the digital realm, where transactions often occur with minimal face-to-face interaction, safeguarding consumer rights takes on new dimensions. The FCCPA empowers consumers by ensuring that they receive fair value for goods and services. It establishes a range of mechanisms for dispute resolution and enforcement through the Competition and Consumer

---

7 Starlion Legal, Legal and Regulatory Framework for setting up an E-Commerce Business in Nigeria, https://starlionlegal.com/2020/10/23/legal-and-regulatory-framework-for-setting-up-an-e-commerce-business-in-nigeria/ > accessed 29th September 2025.

8 Federal Competition and Consumer Protection Act, 2018.

9 Aarndale Solicitors, E-Commerce in Nigeria: Legal Framework and Challenges, Mondaq, https://www.mondaq.com/nigeria/dodd-frank-consumer-protection-act/1465156/e-commerce-in-nigeria-legal-frame work-and-challenges > accessed 29th September 2025.

Protection Tribunal,[10] which provides a structured path for addressing grievances related to unfair practices in the digital space.

The FCCPA is pivotal in regulating e-commerce and digital trade, addressing critical issues such as data privacy, product authenticity, and pricing transparency. With the growth of online shopping platforms, the Act plays a vital role in demanding that businesses adhere to ethical marketing practices and that they maintain high standards of product quality. Moreover, in the context of online transactions, the FCCPA provides a legal framework that promotes the protection of personal information and strengthens consumer confidence in digital platforms.[11] By mandating transparency in terms of business practices, the FCCPA helps to mitigate risks associated with online fraud and deception.

3.2.3. Cybercrime Act 2015

The Cybercrime Act, enacted in 2015, serves as a comprehensive legal framework addressing a wide array of cybercrimes, encompassing online fraud, hacking, identity theft, and cyber-terrorism.[12] The Act's objectives are to prevent and prohibit various types of cybercrime, protect computer systems and networks, and safeguard electronic transactions, while also promoting cybersecurity awareness and international cooperation.[13] The Act also seeks to establish penalties for cybercrime offences and create a safer and more secure online environment for Nigerians, promoting economic growth and development through the safe and secure use of information and communication technologies.[14]

From the objectives of the Act, it can be deduced that this legislation aims to enhance the prevention, detection, investigation, prosecution, and punishment of cyber-related offences in

10 Ibid.
11 Ibid.
12 Cybercrime Act (Prohibition, Prevention etc).
13 Nicholas Idoko, Understanding Nigeria's E-commerce Legislation Landscape, https://professions.ng/e-commerce-legislation/ > accessed 29th September 2025.
14 Ibid.

Nigeria, thereby providing a robust foundation for the security of e-commerce and digital trade.[15] Among its critical provisions, Section 13 delineates the parameters of unauthorised access and manipulation of data. It states:

> A person who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than 7,000,000.00 or both[16]

This provision underscores the importance of maintaining data integrity, particularly for businesses engaged in e-commerce. The Act further defines various cybercrimes and imposes penalties for offences such as identity theft and internet fraud, which pose significant risks to online commerce. By explicitly prohibiting these activities, the Cybercrime Act aims to bolster consumer protection in Nigeria's digital marketplace. Moreover, Section 15 of the Act addresses the unauthorised interception of electronic communications, rendering it illegal to intercept emails, instant messages, or text messages without proper authorisation. This provision highlights the necessity for businesses to safeguard their communication channels against unauthorised access.

To mitigate the risks associated with cyber threats, entities involved in e-commerce and digital trade must proactively secure their computer systems and networks. Compliance with the Cybercrime Act is vital to avoid legal repercussions. Implementing robust password policies and utilising encryption technologies are essential strategies to protect customer data and uphold the integrity of electronic transactions. Accordingly, the effective implementation of the Cybercrime Act is crucial for fostering a secure cyber environment, thereby enhancing

---

15 Ibid.
16 Ibid.

the regulation of electronic transactions in Nigeria.[17] The Act represents a significant achievement in the pursuit of consumer protection and the establishment of a safe framework for e-commerce and digital trade within the country.[18]

3.2.4. Nigerian Data Protection Act[19]

The Nigerian Data Protection Act (NDPA) of 2023 establishes a comprehensive legal framework aimed at protecting personal data within the e-commerce and digital trade sectors. By setting forth stringent guidelines for how businesses can collect, store, and process customer data, the Act prioritises consumer privacy and promotes transparency in online transactions.[20] Key provisions emphasise the necessity for informed consent from customers, the necessity of adhering to purpose limitation, data minimisation practices, and implementing robust data security measures.[21]

Central to the NDPA are the rights afforded to data subjects, which empower customers to access their personal information, rectify inaccuracies, and object to specific types of data processing. This focus on user rights not only fosters trust between consumers and businesses but also underscores the importance of accountability in the digital economy.[22] Additionally, the Act outlines strict requirements for cross-border data transfers, ensuring that any transference of customer data outside Nigeria complies with high data protection standards.[23]

---

17 Kelvin Erue, The Legal Aspects Of E-Commerce And Digital Transactions In Nigeria, AOC Solicitors, https://aocsolicitors.com.ng/the-legal-aspects-of-e-commerce-and-digital-transactions-in-nigeria-kelvin-erue/> accessed 29th September 2025.

18 Ibid.

19 Nigerian Data Protection Act, 2019, <https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf> accessed 29th September 2025.

20 Gabriel Eze, Understanding The Nigeria Data Protection Act 2023: Obligations Of Digital Platforms And Businesses, Mondaq, https://www.mondaq.com/nigeria/privacy-protection/1430338/understanding-the-nigeria-data-protection-act-2023- obligations-of-digital-platforms-and-businesses, (Accessed 20th February 2025)

21 ibid.

22 Ibid.

23 Ibid.

Sections of the NDPA delineate essential principles and obligations for businesses engaged in e-commerce. For instance, Section 24[24] articulates the fundamental principles of data processing, such as data minimisation and purpose limitation, while Section 25 enumerates the lawful bases for data processing. Furthermore, Section 27 mandates that data subjects be informed about the specifics of data collection, including the purpose of processing and their accompanying rights, thereby enhancing transparency.

In cases of data breaches, the NDPA requires businesses to notify affected customers promptly, thereby enabling remedial actions to mitigate potential harm. With provisions that encompass automated decision-making and profiling in Section 37 and guidelines for cross-border data in Section 43, the NDPA provides a robust framework that not only prioritises consumer protection but also positions Nigeria as a leader in the global conversation around data protection and e-commerce. Adhering to these regulations is essential for businesses seeking to thrive in the increasingly complex digital marketplace.[25]

3.2.5. Companies and Allied Matters Act (CAMA) 2020

The Companies and Allied Matters Act (CAMA) 2020 serves as the primary legislation governing the incorporation, regulation, and management of companies in Nigeria. This Act applies to e-commerce and digital trade businesses that are registered as companies in the country. Under CAMA, all companies and businesses are required to comply with the registration regulations outlined in the Act. This includes obtaining a certificate of incorporation,[26] submitting annual returns, and maintaining accurate financial records. CAMA also imposes specific reporting obligations on companies, in which e-commerce and digital trade entities are not left out. These responsibilities include disclosing beneficial

24 Nigerian Data Protection Regulation 2023.
25 Ibid.
26 Section 41 CAMA 2020

ownership and mandatorily filing financial statements.[27] In summary, businesses must adhere to legal formalities and disclose relevant financial information as required by CAMA. Failure to comply may lead to the suspension or revocation of the company's registration, as well as potential fines and other penalties.[28]

3.2.6. The Central Bank of Nigeria (Establishment) Act 2007 and the Banks and Other Financial Institutions Act 2020

The Central Bank of Nigeria (CBN) Act establishes the Central Bank of Nigeria as an autonomous institution tasked with upholding the provisions of the CBN Act and the Banking and Other Financial Institutions Act (BOFIA). One of its primary objectives is to ensure stability in monetary and pricing matters while overseeing a range of financial entities, including banks and related businesses.

In fulfilling its supervisory responsibilities, the CBN is directed by Section 47(2) of the Act,[29] which mandates it to "promote and facilitate the development of an efficient and effective system for the settlement of transactions, including the advancement of electronic payment systems." To this end, the CBN has introduced a series of regulations that are vital to the digital transaction ecosystem, thereby relevant to the promotion of e-commerce and digital trade.[30] These regulations include, but are not limited to: Guidelines on Operations of Electronic Payment Channels (2016). This framework is designed to enhance the development of effective transaction settlement systems, regulating various electronic payment mechanisms such as ATMs, mobile point-of-sale services, and online acceptance

---

27 Section 388 CAMA 2020.
28 Ibid.
29 Central Bank of Nigeria Act 2017 as amended.
30 Ibid.

services.[31] Additionally, it establishes processes for resolving disputes related to the use of electronic payment channels.

Regulation on Electronic Payments and Collections for Public and Private Sectors in Nigeria (2019). This regulation outlines the framework for electronic payment systems utilised by both public and private entities, ensuring secure and efficient transactions across sectors.[32] Therefore, these regulations collectively form a robust legal framework that underpins e-commerce and digital trade in Nigeria, promoting security, efficiency, and reliability in digital transactions.[33]

3.2.7. Sale of Goods Act

The regulation of commercial transactions involving the exchange of goods and services is primarily governed by the Sale of Goods Act. Enacted in 1895 and rooted in English Common Law, this Act, while comprehensive, does not fully address the unique aspects of conducting commercial activities online in the digital age. Nonetheless, it can be argued that online transactions, which constitute contracts for the sale and purchase of goods and services, are still governed by the provisions of this Act.[34]

According to the Act, a contract for the sale of goods involves the transfer, or promise of transfer, of ownership from the seller to the buyer in exchange for a monetary sum referred to as the price.[35] Notably, the Act allows for flexibility in the formation of these contracts;

---

31 Policy Vault, Guidelines on Operations of Electronic Payment Channels in Nigeria, <https://www.policyvault.africa/policy/guidelines-on-operations-of-electronic-payment-channels-in-nigeria/ > accessed 29th September 2025.

32 Central Bank of Nigeria, Regulation on Electronic Payments and Collections for Public and Private Sectors in Nigeria (2019), <https://www.cbn.gov.ng/out/2019/psmd/regulation%20on%20electronic%20payments%20and%20collections.pdf, accessed 29th September 2025.

33 ibid.

34 Muhammad Nuruddeen, Legal Issues in Electronic Commerce: Challenges and Prospects for Nigeria, *ResearchGate,*<https://www.researchgate.net/publication/316736921_Legal_Issues_in_Electronic_Commerce_Challenges_and_Pros pects_for_Nigeria > accessed 29th September 2025.

35 Section 2.

agreements can be made in writing, orally, or through a combination of both.[36] They can also be implied based on the conduct of the parties involved. In the context of e-commerce, this process typically unfolds when a buyer selects an item from an online vendor's catalogue, places an order, and completes payment upon the vendor's acknowledgement and acceptance of that order.[37]

Particularly relevant to e-commerce are the provisions of Section 14 of the Act, which address the significance of product descriptions in sales transactions. This section stipulates that when a sale is predicated on a description, there exists an implied condition that the goods must conform to this description. This legal foundation has been instrumental in fostering consumer protection, as demonstrated by the prevalent #what-i-ordered-vs-what-i-got campaigns on social media, where consumers highlight discrepancies between marketed and delivered products.[38] Thus, while the Sale of Goods Act may be an older piece of legislation, it remains a crucial element in the legal framework governing e-commerce and digital trade.

3.2.8. Standards Organisation of Nigeria Act 1971

The Standards Organisation of Nigeria (SON) Act of 1971 serves as a fundamental legislative framework for regulating product and service standards across various industries in Nigeria. Established with the primary objective of ensuring the quality and safety of goods and services, the SON plays a critical role in both physical and digital marketplaces.[39] With the rapid growth of e-commerce and digital trade, all goods sold online must comply with the standards set forth by the SON.

---

36 Section 4.
37 Ibid.
38 Ibid.
39 Section 4.

In this digital age, businesses engaging in e-commerce must ensure that their products meet the prescribed quality standards to protect consumer rights and maintain healthy competition. The Act mandates that manufacturers and sellers adhere to specific regulations, thereby fostering trust among consumers and promoting fair trade practices[69]. Compliance with these standards not only enhances the reputation of businesses but also safeguards public health and safety, ultimately contributing to the sustainable growth of Nigeria's digital economy[70].

3.2.9. The Evidence Act 2011

Before the 2011 amendment to the Evidence Act, the legitimacy of contracts, particularly in the realm of commercial agreements, faced significant scrutiny in the judicial system. Challenges often arose based on the premise that the prevailing legal framework did not acknowledge the validity of contracts or agreements facilitated through technological means, such as computers and the internet.[40] This was primarily attributed to the absence of established procedures for recognising electronically generated evidence, resolved by the introduction of Section 84 of the Evidence Act 2011. This pivotal provision offers comprehensive guidelines for the recognition and admissibility of electronically generated evidence, thereby affirming the validity of online commercial transactions. The amendment not only enhances the legal clarity surrounding e-commerce but also fosters confidence in digital trade by providing a robust legal framework that supports the seamless integration of technology into commercial practices.

The Evidence Act 2011 is the foundation for recognising electronic records and signatures in Nigerian law. Section 84 establishes the admissibility of electronic records, provided proper certification of authenticity is presented. This means that electronic documents, contracts, and

---

[40] Indira Legal, Legal Framework for the Regulation of E-Commerce and Online Commercial Transactions in Nigeria, <https://indiralegalenquiry.com.ng/legal-framework-for-the-regulation-of-e-commerce-and-online-commercial-transa ctions-in-nigeria/ >accessed 29th September 2025.

communications are admissible in court if the party seeking to rely on them demonstrates that the device or system producing the record was reliable, properly operated, and has not been tampered with.

Section 93(2) expressly validates electronic signatures, providing that "where a rule of law requires a signature, that requirement shall be met in relation to an electronic communication if an electronic signature is used." This statutory recognition is crucial for online contracts, where physical signatures are impractical.

The Nigerian judiciary has affirmed this in several cases. In *Stanbic IBTC Bank v Longterm Global Capital Ltd*,[41] the Court of Appeal upheld the admissibility of electronically generated bank statements as evidence, provided they complied with section 84. Earlier, in *FRN v. Femi Fani-Kayode*[42] the court confirmed that computer-generated evidence is admissible if statutory conditions are satisfied. Although these cases did not specifically involve digital contracts, they demonstrate judicial readiness to treat electronic records as reliable evidence of contractual relations.

Nevertheless, gaps remain. Section 84 has been criticised for imposing overly technical certification requirements, which sometimes hinder admission of electronic evidence. This was highlighted in *Kubor v Dickson*,[43] where failure to produce proper certification led to the rejection of electronic documents. In digital contract disputes, such procedural hurdles may frustrate justice if courts adopt rigid interpretations.

41 (2018) LPELR-CA/L/1095/2016.
42 (2010) 14 NWLR (Pt. 1214) 481.
43 (2013) 4 NWLR (Pt. 1345) 534.

3.2.10. Electronic Transaction Act (ETA)[44]

The Electronic Transaction Act (ETA) serves as a foundational legal framework for e-commerce and digital trade in Nigeria by recognising and validating electronic signatures and transactions. This legislation empowers businesses to conduct commercial activities seamlessly without reliance on traditional paper-based methods.[45]

Key objectives of the ETA encompass the facilitation of electronic commerce and the provision of legal certainty regarding electronic transactions, thereby promoting predictability in the application of the law. Importantly, while the ETA does not mandate the use of electronic transactions, it establishes a comprehensive legal structure for those businesses that opt to engage in digital methods.

The ETA delineates regulations concerning the formation, validity, and enforceability of electronic contracts. Furthermore, it outlines essential disclosure and security requirements for businesses involved in electronic commerce, ensuring that they operate within a secure and transparent environment. This robust framework not only enhances the integrity of digital transactions but also fosters trust among stakeholders in the rapidly evolving landscape of e-commerce.

3.3. Alternative Dispute Resolution (ADR) and Digital Contracts

One of the most practical ways of addressing disputes in digital contracts, especially those with international dimensions, is through Alternative Dispute Resolution (ADR). Litigation, while traditional, is often inadequate for digital commerce disputes due to its rigidity, costs,

---

44 Electronic Transactions Act < https://nass.gov.ng/documents/billdownload/11142.pdf> accessed 30th September 2025.

45 Ibid.

and transnational limitations. ADR methods, particularly arbitration and mediation, provide flexible, private, and more efficient mechanisms.[46]

The Arbitration and Mediation Act (AMA) 2023[47] represents a milestone in Nigeria's dispute resolution framework. It replaced the Arbitration and Conciliation Act 1988 and incorporates modern international best practices, particularly the UNCITRAL Model Law (2006 version)[48] and provisions of the Singapore Convention on Mediation (2019).[49]

Digital contracts demand equally digital means of dispute resolution. ODR is the use of technology to facilitate ADR processes, typically through online platforms.[50] The EU's Regulation (EU) 524/2013[51] established an ODR platform for consumer disputes, allowing parties to submit claims online and resolve them without physical hearings[52]. In Nigeria, ODR is still at a nascent stage[53], but institutions like the Lagos Court of Arbitration (LCA) and the Lagos Multi-Door Courthouse (LMDC) have begun experimenting with online arbitration and mediation, particularly during and after COVID-19 lockdowns.[54]

---

46 Beebeejaun and Faccia, 'Electronic Alternative Dispute Resolution, Smart Contracts and Equity in the Energy Sector', *Journal of World Energy Law and Business,* [2022] (15) 97-113. Available at: < https://pure-oai.bham.ac.uk/ws/portalfiles/portal/188464223/jwac004.pdf> accessed 1st October 2025.

47 <https://ww.ibanet.org/the-nigerian-arbitration-and-mediation-act-2023 > accessed 30th September 2025.

48 UNCITRAL Model Law on International Commercial Arbitration, 1994. < https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-54671_ebook.pdf> accessed 1st October 2025.

49 UN convention on International Settlement Agreements Resulting from Mediation, 2019. <https://uncitral.un.org/sites/uncitral.un.org/files/singapore_convention_eng.pdf > accessed 1st October 2025.

50 Veda Dalvi, 'Online Dispute Resolution (ODR): A Viable Alternative to Court?, *Contractzy,* <https://www.contractzy.io/blog/online-dispute-resolution-odr-a-viable-alternative-to-court > accessed 1st October 2025.

51 < https://eur-lex-europa.eu/eli/reg/2013/524/oj/eng> accessed 1st October 2025.

52 Ibid.

53 O M Atoyebi, 'Online Dispute Resolurion in Nigeria: Trends and Legal Prospects', *Omaplex Law Firm* https://omaplex.com.ng/online-dispute-resolution-in-nigeria-trends-and-legal-prospects/ > accessed 1st October 2025.

54 Lagos Multi Door Court House, < https://lagosmultidoor.org.ng/> accessed 1st October 2025.

3.4. Conclusion

Nigeria's legal framework for digital contracts is evolving but remains inadequate. The Evidence Act 2011, Cybercrimes Act 2015, FCCPA 2018, and CBN guidelines provide fragmented recognition of e-contracts. Nigeria learn from other jurisdictions by adopting harmonised legislation, strengthening consumer protection, and institutionalising ODR. By addressing these gaps, Nigeria can establish a predictable and business-friendly environment for digital contracts, thereby fostering trust, enhancing cross-border trade, and positioning itself as a leader in Africa's digital economy.

CHAPTER FOUR

COMPARATIVE ANALYSIS AND OPPORTUNITIES

4.6. Introduction

The rise of digital commerce has transformed traditional contract law, requiring legal systems worldwide to adapt to electronic transactions. Historically, contracts were made through physical signatures and paper documents in tangible spaces. Today, they are often created in borderless digital environments using electronic signatures, clicks, and algorithms. This change prompts key legal questions: How should "offer" and "acceptance" be defined online? What evidentiary value do electronic signatures carry? How do we determine jurisdiction and applicable law in cross-border deals? And most critically, how can we ensure consumer trust and fairness online? This chapter compares three major jurisdictions: the European Union (EU), the United States (US), and South Africa, each with unique legal traditions and policy approaches. The EU emphasises a unified civil law system focused on consumer protection and cross-border consistency. The US takes a federalist, technologically neutral stance with a focus on arbitration, rooted in common law. South Africa offers a hybrid model combining Roman-Dutch principles with statutory reforms like the Electronic Communications and Transactions Act 2002 (ECT Act). The goal of this comparison is twofold: first, to examine the legal, judicial, and policy responses to digital contracts in these regions; second, to derive ten key lessons for Nigeria, which is still developing its legal framework through laws like the Cybercrimes Act 2015, the Federal Competition and Consumer Protection Act 2018, and the Arbitration and Mediation Act 2023. These lessons highlight areas for reform and opportunities for Nigeria to leverage digital trade within the African Continental Free Trade Area (AfCFTA).

4.7. The European Union

The EU's framework for digital contracts is anchored in harmonisation. The Directive 2000/31/EC on Electronic Commerce (e-Commerce Directive)[1] establishes foundational principles. Article 9 requires Member States to ensure that contracts can be concluded electronically and may not be denied legal effect solely because they are in electronic form. Article 10 further mandates that service providers disclose contractual terms in a clear, comprehensible, and durable format, ensuring transparency for consumers.[2]

Electronic signatures are governed by the eIDAS Regulation,[3] which replaced the earlier Directive 1999/93/EC. Article 25(1) of eIDAS provides that an electronic signature shall not be denied legal effect or admissibility solely because it is electronic. Article 26 distinguishes between "advanced electronic signatures" (AES), which uniquely link to and identify the signatory, and "qualified electronic signatures" (QES), which enjoy the same legal effect as handwritten signatures across all Member States.

Choice of law and jurisdiction in cross-border digital contracts is regulated by the Rome I Regulation[4] and the Brussels I Recast Regulation.[5] Article 3 of Rome I allows party autonomy in choosing applicable law, while Article 6 provides enhanced consumer protection by applying the law of the consumer's habitual residence where contracts are consumer-oriented.

---

1 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Available at: <http://data.europa.eu/eli/dir/2000/31/0j> accessed on 1st October 2025.

2 Ibid.

3 (Regulation (EU) No 910/2014). Available at: <https://digital-strategy.ec.europa.eu/en/policies/discover-eidas> accessed 1st October 2025.

4 (Regulation (EC) No 593/2008). Available at: < https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:177:0006:0016:en:PDF> accessed 1st October 2025.

5 (Regulation (EU) No 1215/2012). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215 > accessed 1st October 2025.

The EU has also pioneered online dispute resolution (ODR) through Regulation (EU) No 524/2013, which established a digital platform for resolving cross-border consumer disputes outside court. This platform reflects the EU's broader policy of accessibility, efficiency, and consumer confidence.[6]

EU courts have clarified these principles in a plethora of cases. In *Content Services Ltd v Bundesarbeitskammer*,[7] the Court of Justice of the European Union (CJEU) held that contractual terms must be made available on a durable medium; merely providing them through a hyperlink on a website was insufficient. This case reinforced transparency obligations.

Also, in *Pammer v Reederei Karl Schluter GmbH*,[8] the CJEU clarified that jurisdiction depends on whether the trader directed commercial activity towards the consumer's Member State. This "targeting test" ensures predictability in online contracts.

In the case of *El Majdoub v CarsOnTheWeb*,[9] the CJEU upheld clickwrap agreements, finding that Article 23 of Brussels I was satisfied where a party had to click "I accept" to access contractual terms. This confirmed the enforceability of online standard-form contracts.

Together, these cases demonstrate the EU's consumer-centric philosophy, requiring both formal validity of e-signatures and substantive fairness in e-contracts.

4.8. The United States

6 Regulation (EU) No 524/2013 of the European Parliament and of the Council. Available at: https://www.legislation.gov.uk/eur/2013/524/introduction/adopted?view=plain > accessed 1st October 2025.
7 (Case C-49/11) [2012] ECR I-0000.
8 (Case C-585/08) [2010] ECR I-12527.
9 (Case C-322/14) [2015] ECR I-0000.

The US employs a dual-layered system, balancing federal uniformity with state autonomy. The Electronic Signatures in Global and National Commerce Act (E-SIGN Act) 2000[10] at the federal level, and the Uniform Electronic Transactions Act (UETA) 1999[11], adopted by most states, are the primary instruments.

Section 101 of the E-SIGN Act, which provides for the general rules of validity of electronic records and e-commerce, also provides that a signature, contract, or other record may not be denied legal effect solely because it is electronic.[12]

Section 7 of UETA echoes this principle at the state level, affirming the equivalence of electronic and written records. It grants legal recognition to electronic records, electronic signatures, and electronic contracts. It states that a record or signature may not be denied legal effect or enforceability simply because it is in an electronic form, ensuring that electronic transactions have the same legal significance as their paper-based counterparts.[13]

Both statutes emphasise technological neutrality, refraining from prescribing specific formats for electronic signatures. Instead, enforceability depends on the intent and consent of the parties.

The US judiciary has played a defining role in shaping e-contract enforceability, particularly with respect to shrinkwrap, clickwrap, and browsewrap agreements.[14] In *ProCD v*

---

10 Electronic Signatures in Global and National Commerce Act, 115 STAT. 464 2000. Available at: < https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf> accessed 1st October 2025.

11 Uniform Electronic Transactions Act, 1999. Available at: < https://www.uaipt.com/uploads/legislacion/files/0000004550_UNIFORM%ELECTRONIC%20-TRANSACTIONS%20ACT.pdf> accessed 1st October 2025.

12 Ibid.

13 Edoc Innovations, 'Electronic Transactions Act Summary' <http://www.uniformlaws.org/ActSummary.aspx.?title=Electronic%20Transactions%20Act > accessed 1st October 2025.

14 Barry Werbin, 'Ensuring Enforceability of Online E-Commerce Agreements', *NYSBA Inside* [2016] (34) (1) 45-52. Available at: <https://www.herrick.com/content/uploads/2016/06/Ensuring-Enforceability-of-online-E-commerce.pdf> accessed 1st October 2025.

Zeidenberg,[15] the court upheld shrinkwrap licences, ruling that consumers are bound by terms enclosed with software packaging, provided they had the opportunity to reject the product.

Also, in *Specht v Netscape Communications Corp*,[16] however, the court refused to enforce terms that were hidden below the download button, holding that consent requires reasonably conspicuous notice.

In *Nguyen v Barnes & Noble Inc.,*[17] the Ninth Circuit reaffirmed that browsewrap agreements, where terms are available only through a hyperlink, are unenforceable unless the user has actual or constructive notice.

The US Supreme Court has also reinforced arbitration in digital contracts. In *AT&T Mobility LLC v Concepcion,*[18] the Court upheld mandatory arbitration clauses in consumer contracts, even when they barred class actions, emphasising the pro-arbitration policy of the Federal Arbitration Act (FAA).

This reflects the US preference for enforcing contractual autonomy, albeit tempered by minimum notice and consent standards.

4.9. South Africa

South Africa provides an African model of electronic contract regulation through the Electronic Communications and Transactions Act.[19]

Section 11(1) affirms that information in the form of data messages must not be denied legal effect, validity, or enforceability solely because it is wholly or partly in the form of a data message.

---

15 (86 F.3d 1447, 7th Cir. 1996).
16 (306 F.3d 17, 2d Cir. 2002).
17 (763 F.3d 1171, 9th Cir. 2014).
18 (563 U.S. 333, 2011).
19 Act No 25 of 2002 (ECT Act). Available at: <https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf> accessed 1st October 2025.

Section 13 recognises electronic signatures, distinguishing between ordinary electronic signatures and "advanced electronic signatures" accredited by the Department of Communications. Section 22 provides that contracts formed electronically are valid unless otherwise excluded by law. Consumer protection is further provided under the Consumer Protection Act 68 of 2008 (CPA), which regulates unfair contract terms, disclosure obligations, and remedies for defective goods. Importantly, Section 48 prohibits suppliers from imposing unfair, unreasonable, or unjust contract terms, which applies equally to digital contracts.

South African courts have pragmatically interpreted the ECT Act. In *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd*,[20] the Supreme Court of Appeal held that emails containing the parties' typed names constituted valid electronic signatures under Section 13(3) of the ECT Act. This case underscored flexibility in recognising electronic signatures. In *Jafta v Ezemvelo KZN Wildlife*,[21] the Labour Court held that emails exchanged between employer and employee constituted binding agreements, reaffirming Section 11 of the ECT Act.

These cases demonstrate South Africa's commitment to functional equivalence, recognising electronic records as substantively equivalent to traditional contracts while embedding strong consumer protection.

4.10. Lessons for Nigeria

The comparative analysis yields ten critical lessons for Nigeria as it develops its regulatory framework for digital contracts:

1. Like the EU's eIDAS Regulation and South Africa's ECT Act, Nigeria requires a unified Electronic Transactions Act to consolidate fragmented provisions in the

[20] [2015] ZASCA 178.
[21] [2008] ZALC 21.

Cybercrimes Act 2015, sectoral banking regulations, and the Evidence Act 2011.[22] A single comprehensive statute would enhance legal certainty.

2. Section 17 of the Cybercrimes Act recognises e-signatures, but Nigeria should emulate South Africa's Section 13 ECT Act by distinguishing between ordinary and advanced electronic signatures. This two-tier model provides flexibility while ensuring authenticity in high-value transactions.
3. The EU's Article 10 e-Commerce Directive and South Africa's Section 48 CPA highlight the need for transparency and fairness. Nigeria's Federal Competition and Consumer Protection Act 2018 should be expressly extended to digital contracts, mandating disclosure and prohibiting unfair terms.
4. US precedents such as *Specht v Netscape* and *Nguyen v Barnes & Noble* show the importance of judicial standards for online consent. Nigerian courts should develop jurisprudence clarifying the enforceability of clickwrap and browsewrap agreements to protect consumers.
5. The EU's Rome I Regulation offers a template for balancing party autonomy and consumer protection. Nigeria should codify conflict-of-laws rules specific to digital contracts to reduce uncertainty in cross-border e-commerce.
6. The EU's ODR Regulation 524/2013 and Singapore's adoption of digital arbitration provide a roadmap. Nigeria should operationalise ODR mechanisms under the Arbitration and Mediation Act 2023, offering low-cost, efficient dispute resolution.
7. The US approach in *AT&T Mobility v Concepcion* shows arbitration's role in managing mass consumer disputes. Nigeria can encourage arbitration clauses in digital contracts, balanced by safeguards against unfair exclusion of consumer remedies.

---

[22] Sections 84 to 89, Evidence Act 2011 (as amended 2023).

8. Indian and South African precedents stress flexibility in admitting electronic records. Nigerian courts should liberally interpret Section 84 of the Evidence Act 2011, recognising metadata, emails, and digital logs as valid evidence in contract enforcement.
9. The EU's "qualified trust service providers" and South Africa's accreditation of advanced signatures illustrate the need for institutional support. Nigeria should strengthen the National Information Technology Development Agency (NITDA) as the certifying authority for digital signatures.
10. Nigeria should harmonise domestic law with AfCFTA protocols on digital trade, drawing lessons from the EU's regional harmonisation. This will enhance Nigeria's competitiveness and leadership in Africa's digital economy.

4.11. Conclusion

The comparative analysis reveals contrasting yet complementary approaches. The EU prioritises consumer confidence through harmonisation, transparency, and ODR. The US prioritises enforceability and arbitration, tempered by minimum notice and consent standards. South Africa provides a pragmatic African adaptation, embedding functional equivalence and consumer protection in statutory form. For Nigeria, the central opportunity lies in synthesising these models: adopting the EU's consumer focus, the US's technological neutrality, and South Africa's pragmatic flexibility. By doing so, Nigeria can establish a coherent, trusted, and globally competitive digital contract regime, capable of driving economic growth and positioning the country as a leader in AfCFTA digital future.

CHAPTER FIVE

SUMMARY, RECOMMENDATIONS AND CONCLUSION

5.4. Summary

The introductory chapter provided a conceptual basis for the study by defining digital and electronic contracts as agreements created through electronic means such as email, click-wrap, browse-wrap, or other technological platforms. It discussed how the rise of e-commerce and digital transactions has challenged traditional contract law, which is rooted in common law principles like offer, acceptance, consideration, and the intent to create legal relations. In Nigeria, this shift offers both opportunities and legal challenges, requiring the legal system to adapt to a borderless digital economy while protecting consumers and ensuring commercial certainty.

Chapter Two examined the legal theories and technological frameworks of digital contract formation. It reaffirmed that classical principles like offer and acceptance are applicable online but need contextual adaptation. Nigerian contract law, influenced by English common law and partly codified in the Contract Law of Lagos State 2011, recognises an agreement binding once there is consensus ad idem. Online, this is often shown through clicking an "I agree" button (clickwrap) or conduct (browsewrap). Cases such as *Specht v Netscape Communications Corp.*[23] emphasise notice and consent, while the CJEU upheld clickwrap agreements in *El Majdoub v CarsOnTheWeb*.[24] Electronic signatures are recognised in Nigeria under Section 17 of the Cybercrimes Act 2015, but lack the detailed distinctions seen in the EU's eIDAS Regulation (2014) or South Africa's ECT Act 2002. Technological innovations like blockchain-based smart contracts were discussed as emerging legal challenges. The chapter concluded that Nigerian law remains fragmented and reactive,

[23] (306 F.3d 17, 2d Cir. 2002).
[24] (Case C-322/14) [2015] ECR I-0000.

needing reform to align with the functional equivalence principle from UNCITRAL's Model Law on Electronic Commerce.

Chapter Three evaluated Nigerian laws in regulating digital contracts. It pointed out that Section 84 of the Evidence Act 2011 admits electronic records as evidence if proven authentic, but imposes technical hurdles that might hinder legitimate e-contract proof. The Cybercrimes Act 2015 was analysed for its provisions on e-signatures and cybersecurity, but criticised for emphasising cybercrime control over commercial regulation. The Federal Competition and Consumer Protection Act 2018 (FCCPA) was noted as a framework that could extend consumer protection to digital contracts, though its application is still developing. Nigerian case law on e-contracts is limited. Challenges include the lack of comprehensive legislation, unclear choice of law for cross-border contracts, weak institutions, low consumer awareness, and the absence of online dispute resolution mechanisms.

Overall, Nigeria's legal framework is fragmented, reactive, and not fully aligned with international standards. Chapter Four analysed digital contract laws in the EU, the US, and South Africa to draw lessons for Nigeria. The EU's harmonised approach, through directives like the e-Commerce Directive 2000/31/EC, the eIDAS Regulation 2014, and the Rome I Regulation 593/2008, balances party autonomy with consumer protections and cross-border dispute resolution. Key cases such as *Pammer v Reederei Karl Schluter GmbH*[25] and *Content Services Ltd v Bundesarbeitskammer*[26] underscore this focus. The US approach, via the E-SIGN Act 2000, UETA 1999, and cases like *ProCD v Zeidenberg*[27] and *AT&T Mobility LLC v Concepcion*,[28] emphasises technological neutrality, enforceability, and arbitration. South Africa, through the ECT Act 2002 and the Consumer Protection Act 2008, offers an African

[25] (C-585/08) [2010].
[26] (C-49/11) [2012].
[27] (86 F.3d 1447, 7th Cir. 1996).
[28] (563 U.S. 333, 2011).

model of functional equivalence, affirmed in *Spring Forest Trading v Wilberry*,[29] where typed names in emails were validated as e-signatures.

5.5. Recommendations

1. Nigeria should enact a dedicated statute, similar to South Africa's ECT Act 2002 and the EU's eIDAS Regulation, consolidating provisions on electronic signatures, electronic records, consumer protection, and ODR. This Act should adopt UNCITRAL's Model Law on Electronic Commerce (1996) as its foundation, ensuring international compatibility.
2. Section 17 of the Cybercrimes Act 2015 should be amended to distinguish between ordinary electronic signatures and advanced electronic signatures, akin to Section 13 of South Africa's ECT Act 2002. This two-tier system will allow flexibility for low-value contracts and security for high-value transactions, enhancing trust.
3. The FCCPA 2018 should be explicitly amended to cover digital contracts, requiring full disclosure of terms, prohibiting unfair clauses, and mandating cooling-off periods for online consumer contracts.
4. Nigeria should legislate rules based on the EU's Rome I Regulation, allowing parties to select applicable law while protecting consumers through default rules linking contracts to the consumer's habitual residence or place of performance. This will address uncertainty in cross-border disputes.
5. The Arbitration and Mediation Act 2023 should be implemented with an online dispute resolution platform. This will reduce court congestion, lower transaction costs, and provide small businesses and consumers with accessible remedies.

[29] (2015) ZASCA 178.

6. Nigeria should promote arbitration clauses in digital contracts while safeguarding consumers against unconscionable exclusions of remedies. The Arbitration and Mediation Act 2023 provides a modern framework to achieve this balance.
7. Nigerian courts should draw on US precedents like *Specht v Netscape* and *Nguyen v Barnes & Noble* to develop clear standards distinguishing enforceable clickwrap agreements (with explicit consent) from unenforceable browse-wrap agreements (with hidden terms). This will enhance predictability.
8. Section 84 of the Evidence Act 2011 should be interpreted or amended to reduce onerous certification requirements for electronic evidence.
9. The National Information Technology Development Agency (NITDA) should be empowered as a certifying authority for digital signatures, following the EU's qualified trust service providers model. Investment in technical infrastructure and training for judges and regulators is critical.
10. Nigeria should harmonise its digital contract laws with AfCFTA Protocols on E-Commerce, just as the EU harmonised its internal market. This alignment will expand Nigeria's role in Africa's digital economy, facilitating cross-border trade and positioning it as a hub for digital commerce.

5.6. Conclusion

This study shows that regulating digital and electronic contracts in Nigeria is both urgent and presents a significant opportunity. The five chapters reveal that while Nigerian law generally accepts electronic contracts and signatures, it remains fragmented, underdeveloped, and reactive to technological advances. Judicial decisions are limited, laws are scattered, and consumer protection in digital spaces is weak. Without reforms, these issues will continue to undermine trust, slow e-commerce, and restrict Nigeria's role in global and regional digital economies. Insights from the EU, US, and South Africa offer helpful guidance: the EU

emphasises harmonisation, consumer protection, and ODR; the US highlights neutrality, enforceability, and arbitration; South Africa provides a practical African model focusing on functional equivalence and fairness. Nigeria's chance is to combine these approaches into a unique model that fits domestic realities while adopting the best international practices. Ultimately, regulating digital contracts is more than a technical matter; it's a policy priority impacting economic growth, consumer trust, judicial efficiency, and Nigeria's global competitiveness. By passing laws, building institutional capacity, including consumer protections, and aligning with AfCFTA general and specific objectives, Nigeria can develop a robust digital contract framework that supports inclusive growth. The future success of Nigeria's digital economy depends on legal clarity, fairness, and trust- elements that effective regulation can ensure.

BIBLIOGRAPHY

Books

Peel's Treitel E.*: The Law of Contract,* 12th edn. 2010

Sagay's I. E. *Nigerian Law of Contract,* 2nd edn. 1999 pg 20

Todd's E. Gringras: *The Laws of the Internet*, 3rd edn. 2008 at pg. 25.

Treitel*: The Law of Contract*, 12 edn. 2010

Journals

Akanbi M. M.et al, "An Appraisal of the Nigerian Advance Fee Fraud and Other Fraud Related Offences Act 2006," *The Nigerian Law Journal,* Vol. 16 No. 1 (2013), p. 126.

Castellani L., "The United Nations Electronic Communications Convention – Policy Goals and Potential Benefits," 19(1) *Korean Journal of International Trade and Business Law*, Vol. 1 (2010), p. 2.

Christensen S., "Formation of Contract by Email- Is it Just the Same as the Post", *QUTLJ,* [2001] (1) (1) 25.

Omaplex Law Firm, *Understanding Smart Contracts: Legal Implications, Benefits, and Challenges in Nigeria*, July 2025.

Peel's Treitel E.*: The Law of Contract,* 12th edn. 2010.

Udoma Udo & Belo-Osagie, *Smart Contracts: Legal Implications in the Nigerian Capital Market*, August 2024.

Umezuruike H. A. C., "Electronic Bills of Lading, Rotterdam Rules and the Nigerian Evidence Act," *The Nigerian Law Journa*l, Vol. 16 No. 1 (2013), p. 71.

Online Contents

Aarndale Solicitors, E-Commerce in Nigeria: Legal Framework and Challenges, Mondaq, https://www.mondaq.com/nigeria/dodd-frank-consumer-protection-act/1465156/e-commerce-in-nigeria-legal-frame work-and-challenges > accessed 29th September 2025.

Akinpelu A.O., Legal Issues in Regulating the E-commerce Sub-Sector in Nigeria, <https://www.scribd.com/document/333534315/Legal-Issues-in-Regulating-the-E-commerce-Sub-sector-in-Nigeria> accessed 29th September 2025.

Atoyebi O M, 'Online Dispute Resolurion in Nigeria: Trends and Legal Prospects', *Omaplex Law Firm* https://omaplex.com.ng/online-dispute-resolution-in-nigeria-trends-and-legal-prospects/ > accessed 1st October 2025.

Beebeejaun and Faccia, 'Electronic Alternative Dispute Resolution, Smart Contracts and Equity in the Energy Sector', *Journal of World Energy Law and Business,* [2022] (15) 97-113. Available at: < https://pure-oai.bham.ac.uk/ws/portalfiles/portal/188464223/jwac004.pdf> accessed 1st October 2025.

Dalvi Veda, 'Online Dispute Resolution (ODR): A Viable Alternative to Court?, *Contractzy,* <https://www.contractzy.io/blog/online-dispute-resolution-odr-a-viable-alternative-to-court > accessed 1st October 2025.

Erue Kelvin, The Legal Aspects Of E-Commerce And Digital Transactions In Nigeria, AOC Solicitors, https://aocsolicitors.com.ng/the-legal-aspects-of-e-commerce-and-digital-transactions-in-nigeria-kelvin-erue/> accessed 29th September 2025.

Ewelukwa N., "Is Africa Ready for Electronic Commerce? A Critical Appraisal of the Legal Framework for Ecommerce in Africa" available at http://www.acicol.com/__temp/Dr_N.pdf accessed 20th September 2025.

Eze Gabriel, Understanding The Nigeria Data Protection Act 2023: Obligations Of Digital Platforms And Businesses, Mondaq, https://www.mondaq.com/nigeria/privacy-protection/1430338/understanding-the-nigeria-data-protection-act-2023- obligations-of-digital-platforms-and-businesses, (Accessed 20th February 2025)

Idoko Nicholas, Understanding Nigeria's E-commerce Legislation Landscape, https://professions.ng/e-commerce-legislation/ > accessed 29th September 2025.

John S. Foster, "Electronic Contracts and Digital Signatures," available at http://www.corbinball.com/articles_legal/index.cfm?fuseaction=cor_av&artID> accessed 29th September 2025. see also Victor Chandler International v. Customs &Excise Commissioners [2000] 1 WLR 1296 where it was held that electronically stored information can in law constitute a document.

Nuruddeen Muhammad, Legal Issues in Electronic Commerce: Challenges and Prospects for Nigeria, *ResearchGate,*<https://www.researchgate.net/publication/316736921_Legal_Issues_in_Electronic_Commerce_Challenges_and_Pros pects_for_Nigeria > accessed 29th September 2025.

Rothchild J. A., "Consumer Protection and the Internet," in Handbook of Research on International Consumer Law, G. Howells et al eds. (UK: Edward Elgar Publishing Ltd., 2010), p. 344.

Starlion Legal, Legal and Regulatory Framework for setting up an E-Commerce Business in Nigeria, https://starlionlegal.com/2020/10/23/legal-and-regulatory-framework-for-setting-up-an-e-commerce-business-in-nigeria/ > accessed 29th September 2025.

Werbin Barry, 'Ensuring Enforceability of Online E-Commerce Agreements', *NYSBA Inside* [2016] (34) (1) 45-52. Available at: <https://www.herrick.com/content/uploads/

2016/06/Ensuring-Enforceability-of-online-E-commerce.pdf> accessed 1st October 2025.