REGULATION OF ELECTRONIC CONTRACTS IN NIGERIA AND SOUTH AFRICA: A COMPARATIVE ANALYSIS

Uju Obuka*

Abstract

This paper appraises the legal regime for electronic contracts in Nigeria and South Africa. The paper finds that South Africa has one of the best legal frameworks for electronic transactions in the world and that contrary to the position in South Africa, there is no specific legislation on electronic contracts presently in Nigeria, instead the courts in Nigeria have continued to adopt liberal interpretation to the existing contract and commercial laws to accommodate electronic transactions in Nigeria. The paper contends that the successes recorded in electronic transactions in South Africa are attributable to a well-articulated legal regime and Nigeria should adopt the position in South Africa. The paper employs doctrinal methodology with analytical and comparative approaches. The necessity of establishing the accuracy of the findings on the inevitability of enacting a comprehensive law on electronic transactions like that of South Africa is the justification for using the method. The paper concludes by making a case for the outright enactment of the Electronic Transactions Bill into law.

Keywords: Electronic contract, Nigeria, South Africa, Electronic Communications and Transactions Act, Electronic Transactions Bill

Introduction

Hitherto, the law revolved around physical objects. Tangible goods are bought and sold, and information and content are distributed on paper. There is typically something tangible delivered from seller to buyer. Likewise, the medium of commerce is a tangible object i.e. a paper.[1] Activities that, before the computer age, took place only in the physical spheres like land, air, and sea are now taking place over cyberspace and are governed by laws made to handle the peculiar nature of those spaces.[2] Today, those realities have been fundamentally altered. The internet and computers have virtually taken over most of the functions being undertaken in actual reality. The emergence of the internet over the last couple of years as an important tool for the conduct of business and other social functions has created a yearning gap in our legal system necessitating that laws be put in place to cater to electronic-related activities, or that the existing laws be amended or adapted to conform with advancements in modern technology.

Many advanced countries of the world have long enacted their respective cyber laws following the United Nations Convention on International Trade Law (UNCITRAL) Model Law on E-commerce which was enacted to serve as a guide to nations to come up with legislation that will give legal recognition to online transactions.[3] For instance, South Africa enacted the Electronic Communications and Transactions Act (ECTA) in 2002. The ECTA[4] has been adjudged one of the best in the world as far as electronic transactions are concerned. Apart from providing for the legal recognition of online contracts, admissibility of electronic documents, data protection, protection of consumers of online goods and services as well as the provision of mechanisms for checking cybercrimes, it is the first legislation to provide for the exact moment an electronic

* **Uju Obuka, Ph.D., LL.M, BL, LL.B, Senior Lecturer in Law, Faculty of Law, University of Nigeria Nsukka. uju.obuka@unn.edu.ng. Contact: 08033280467.**

1 T Smedinghoff, 'Online Law: What's New and Different' in T J Smedinghof (ed), *Online Law: The SPA'S Legal Guide to Doing Business on the Interne* (Addison – Wesley Developers Press 1996), 3.

2 Banwo & Ighodalo, 'Milestone in Electronic Commerce: How the Cybercrimes Act 2015 Impacts Businesses' <https://www.banwo-ighadalo.com.> accessed 16 June 2023

3 See UNCITRAL Model Law on Electronic Commerce 1996 with additional art.5bis adopted in 1998 General Assembly Resolution 51/162 of 16 December 1996 <https:// www.uncitral.org.> accessed 20 June 2023.

4 25 of 2002.

contract would be deemed to have come into existence. The same cannot be said about Nigeria which has not done anything serious since 2015 when the Nigeria Electronic Transactions Bill was curled from the ECTA of South Africa. This invariably has accounted for the uncertain legal environment concerning online transactions in Nigeria. It is in this context that this paper advocates the enactment of electronic transactions law as obtainable in South Africa to accord legal recognition to electronic contracts in Nigeria. The paper is divided into four parts. Part one is the general introduction and it gives the background to the paper. Part two deals with the legal regime for electronic contracts in Nigeria. Part three focuses on the legislative framework for electronic contracts in South Africa and lessons for Nigeria. Part four is the concluding part and makes a case for the adoption of the position in South Africa to boost electronic contracts in Nigeria.

Legal Regime for Electronic Contracts in Nigeria

There is no specific law yet for the regulation of electronic contracts presently in Nigeria but, significant efforts have been made at legislating for electronic transactions in Nigeria. Aside from that, the extant contract laws have been adapted for use in electronic contracts. This subhead is dedicated to showing the lacuna in the present legislation that has necessitated the enactment of comprehensive legislation to govern electronic contracts in the country.

The Old Era

In Nigeria, a contract is regulated by the contract law of the different states.[5] The said laws provide for the rights, obligations, and liabilities of parties to the contract. Equally, the laws provide that a contract may be entered into in writing, orally, or by conduct. Section 6 of the Enugu State Contract Law for instance provides:

> Subject to this part of the law and any other written law from time to time in force in the state, there shall be no legal requirements as regards form for a valid contract, and so a contract may be made orally, or in writing without seal or by deed.[6]

Although the above-mentioned section says that there shall be no legal requirements as regards the form for a valid contract, it went ahead to stipulate the forms a contract may take. It may be made orally, in writing without seal, or by deed. A critical appraisal of the modes of entering into contracts stipulated by the above provision will reveal that only the traditional means of contracting are envisaged, and the parties to the contract must transact in the presence of each other. Writing in the context used in the laws connotes inscriptions on tangible substances, and the conduct of the parties can be deduced from the previous course of dealings between the parties. Thus one can say with reasonable certainty that the framers of the extant laws on contract had paper-based contracts in mind when they fashioned the laws. It would not be surprising to conclude so because computers and related devices were not in existence at the time the laws were enacted. Nowadays, computers and related devices have overtaken most of the functions being performed by human beings with the result that computers and related devices are now employed in the formation of contracts. This state of affairs implies that the status of contracts entered into using these technological advances is not certain as far as the existing contract laws are concerned in Nigeria.

Even admitting those contracts into proceedings was fraught with a lot of challenges, ranging from determining whether those pieces of evidence qualify as documentary evidence, and if they do, whether they should be classified as primary or secondary evidence. Most computer-generated evidence was denied admissibility on account of the uncertainty of their status under our law. This problem was heightened by the fact that the definition of documents under the old Evidence Act did not incorporate electronic impulses or data messages.

---

5 See for example, Law Reform (Contracts) Law Cap L 81 Laws of Lagos State 2015, Contract Law Cap 26, Revised Laws of Enugu State 2004, and Contract Law Cap 32 Laws of Anambra State 1991.

6 Contract Law Cap 26, Laws of Enugu State 2004.

Section 2 of the Act defined document as:
Books, maps, plans, drawing, photograph, and also includes any matter expressed or inscribed upon any substance by means of letters, figures, or marks or by more than one of these means intended to be used or which may be used for the purpose of recording that matter. [7]

A careful analysis of the above section will reveal that no amount of stretching or interpretation will bring in computers and related devices within the purview of this definition. This therefore accounted for why most courts were reluctant to admit computer-generated evidence under the old Evidence Act. This reluctance on the part of the court and the lack of specific legislation on electronic transactions created an unpredictable legal landscape for electronic contracts in Nigeria, which invariably reduced the volume of electronic transactions in the country. The frustration encountered in handling new technological advances in Nigeria led to the formulation of a law that will promote the use of information technology in Nigeria.

National Information Technology Development Agency Act 2007

The earliest recognition of the necessity to regulate electronic transactions in Nigeria started with the enactment of the National Information Technology Development Agency Act.[8] The major objective of the Act is the establishment of the National Information Technology Development Agency to plan, develop, and promote the use of information technology in Nigeria. A careful analysis of the responsibilities of the agency will reveal that the agency was set up to promote and encourage the use of information technology in Nigeria, and to play an advisory and supervisory role as far as information technology is concerned. The Act falls short of providing for the regulation of electronic contracts and other related transactions. This shortcoming necessitated the need to enact laws that would regulate electronic transactions in Nigeria.

Electronic Transactions Bill of 2015

The enactment of the National Information Technology Development Agency Act ushered in a new phase in the enactment of legislation to regulate electronic transactions in the country. However, most of these efforts are in the stages of draft bills pending before the National Assembly.[9] The most significant of these Bills and relevant to the regulation of electronic contracts is the Electronic Transactions Bill of 2015. The Bill was passed by the National Assembly on 3 June 2015, and it has not been assented to as at the time of writing this article. The Bill provides for the validity of contracts, matters of evidence, data protection, consumer protection, electronic signatures, and payment systems, amongst other issues. Highlighting the advantages of the Bill, Aniaka had this to say

> The Bill is remarkable in that, it is an attempt to deepen the benefits derivable from electronic transactions and address, as much as possible, certain legitimate concerns about electronic transactions in Nigeria, such as non-disclosure of full information on products and services, deceptive advertisement, improper description of products, delivery of defective products, poor informal dispute settlement procedures, double payments and poor customer service.[10]

---

7 Evidence Act Cap E14, LFN 2004 s 2.

8 (NITDA) Act No 60 2007.

9 These Bills include; Electronic Transactions Bill of 2015, National Internal Security Bill of 2009, Security Communications Interception and Monitoring Bill of 2009, Critical Infrastructure Protection Bill of 2009, Computer Security & Protection Bill of 2009, Electronic Commerce (Provision of Legal Recognition) Bill of 2008, Electronic Fraud (Prohibition) Bill of 2008, Nigerian Antitrust (Enforcement, Miscellaneous Provisions etc.) Bill of 2008, Cyber Security and Data Protection Agency (Establishment) Bill of 2008.

10 See O Aniaka, 'Analyzing the Adequacy of Electronic Transactions Bill 2015 in Facilitating E-commerce in Nigeria' <https://www.ssrn.com.> accessed 16 June 2023.

Analysis of the Bill

The Bill provides that no information shall be denied legal effect, validity, or enforcement solely on the ground that it is in electronic form.[11] However, the effectiveness of such information is not affected by the location where the information was created or used or by the place of business of its creator.[12] Again the Bill provides that electronically generated documents are admissible if the document met the reliability test. Furthermore, the Bill provides that the use of electronic material is not mandatory. Thus, consent is required to use electronic material.[13]

Again the Bill provides that electronic information is an original document and satisfies the requirement of writing if the following criteria are met:

(i) That information must be accessible to be usable for subsequent reference;
(ii) The information is capable of being retained by the person to whom it is given;
(iii) Where a form is prescribed, the information in electronic form is organized in the same or substantially the same form.[14]

However, the integrity of the information provided in such electronic form is maintained only if, the information remains complete and unaltered save for any endorsement thereon or changes that arise in the normal course of communication, storage, or display. The combined effects of s. 4 (1) (3) and s.6 of the Bill is that the requirements of writing, signature, and prescribed form are deemed to be complied with when done electronically and, electronic records or data messages qualify as original documents.

Section 11 of the Bill provides for the validity of electronic signatures. It provides that:

(a) Where the signature of a person is required, that requirement is met in relation to an electronic communication, if any method is used to identify the person and to indicate the person's approval of the information communicated;
(b) Having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated; and
(c) The person to whom the signature is required to be given, consents to that requirement being met by way of the use of the method mentioned in paragraph (a).

To ensure the authenticity and integrity of electronic signatures, section 13 provides for electronic signature/certification services to be provided by a Certification Authority in accordance with the provisions of the accreditation granted under the electronic signature administration. Thus only a certified electronic signature will be admitted as a genuine signature.

Section 17 combined with s 35 (1) provides for the protection of personal data. Thus, personal data shall only be processed if, at least one of the following conditions is met:

The data owner has given his consent to the processing;
The processing is necessary for the performance of a contract to which the data owner is a party, or for the taking of steps at the request of the data owner, with a view to entering into a contract;
The processing is necessary for compliance with any legal obligation to which the data holder is subject, other than an obligation imposed by contract;
The processing is necessary in order to protect the vital interests of the owner;

[11] Electronic Transaction Bill s 3.
[12] S 10.
[13] S 14.
[14] S 4 (1) & (3) 6.

The processing is necessary in the interests of the public and good governance.

By s 17 (5) & (7) personal data processed for whatever purpose will not be kept longer than is necessary and, shall not be transferred to a foreign country unless the foreign country has an adequate level of protection for the rights and freedom of data owners concerning the processing of personal data. S 35 (1) mandates service providers or vendors to ensure the confidentiality of all personal information collected from the consumer, except where the consent of the consumer is obtained or where the law demands disclosure.

Section 26 provides for the validity of electronic contracts. It provides that:

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and acceptance may be expressed by means of a document as defined in this Act.
(2) Where a document is used in the formation of a contract, the contract shall not be denied validity or enforceability on the ground that an electronic document was used for that purpose.
(3) A contract may be formed by the interaction of electronic agents, provided that the interaction results in the agents engaging in operations that confirm or indicate the existence of a contract.

Section 33 provides for the protection of consumers of goods and services. By Sub-section (1) providers of services or vendors shall provide a consumer with sufficient and relevant information to enable informed decisions on the part of that consumer. Section 35 (2) mandates service providers or vendors to make their privacy policy public and easily accessible to the consumer before the commencement of the contract, and whenever personal information is either requested or collected. Equally, Section 36 mandates service providers or vendors to prominently display a return address and, clearly provide a simple procedure by which a consumer can notify the sender that he does not wish to receive unsolicited electronic message.

Shortcomings of the Bill

The above-mentioned objectives and provisions are laudable and will boost electronic contracts if enacted into law. However, the Bill is not without shortcomings. The shortcomings relate to the following:

(i) The Exact Time a Contract comes into Existence

The Bill provides for the formation of contracts using electronic communication, and that such contracts are valid and enforceable if the conditions stipulated in the Bill are met.[15] However, the Bill does not provide for the exact time a contract can be said to have come into existence, and whether the display of goods on online platforms amounts to an offer or an invitation to treat. The Bill also does not state when an email offer will be deemed to have been made. Issues bordering on legal principles of offer and acceptance have been the subject of several judicial pronouncements, and clarity is desired concerning how they apply in online transactions.[16]

(ii) Non-Delivery of Goods and Services

Another shortcoming of the Bill is the issue of non-delivery of goods and services which have been paid for. One of the major highlights of the Bill is the provision requiring the vendors of goods and providers of services to disclose information about themselves, the goods, and the details of the transaction. However, there is no corresponding provision addressing the issue of

[15] Ss 26-29.
[16] Aniaka (n 10).

non-delivery of goods that have been paid for. This is a major flaw because it gives room for obvious evasion of liability on the part of the online merchant.[17]

(iii) No Guarantee of the Safety of Electronic Payment System

While the Bill makes provision for payments to be made by electronic means, it does not provide a guarantee as to the safety or security of making payment by such means. However, as noted above, the Cybercrimes Act deals with matters relating to cyber security and should be read together with the Bill, when passed into law.[18]

(iv) Enforcement and Conflict of Laws

Conflict of laws is the main issue with contracting with parties from different countries. The Bill provides for the time an electronic communication is deemed to be sent when it is deemed to be received, and from where it is deemed to be sent and received. The Bill is however silent on what happens where the only address provided is an email address, and which law will apply to the transaction? Which court has jurisdiction to entertain any dispute that may arise between the parties? This uncertainty in the law needs urgent attention and amendment because a law needs to be definite in its provisions.

(v) Specialized Courts and Tribunals

Electronic Transactions Bill failed to recognize that electronic transactions are intricate areas that require specialized practitioners and tribunals to handle the complex issues that are bound to erupt in the relationship between the parties and provide for special courts or tribunals that will entertain disputes whenever they arise in electronic transactions. The Bill also did not provide for specialized training for the personnel that will Mann these courts and tribunals. This is a serious issue that needs to be tackled. It is submitted that if these shortcomings are tackled, the Bill when enacted into law will be an all-encompassing legal instrument for the regulation of electronic transactions in Nigeria.

Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes (Prohibition, Prevention, etc.) Act is the first of its kind in Nigeria, as this was the first time legislation was provided strictly for cybercrimes. A precursor of the Act; the Telecommunications and Postal Offences Act,[19] applies mainly to telecommunications and postal offences even though it provides punishment for any person who engages in computer fraud or does anything relating to fake payments, whether or not the payment is credited to the account of an operator or the account of a subscriber. Judging from the objectives of the Telecommunications and Postal Offences Act, it is not strictly for the regulation of cybercrimes.

Equally, the Advance Fee Fraud and Other Fraud Related Offences Act[20] prescribes punishment for any person who engages in fraudulent activity but is not strictly for cybercrimes. The increase in online activities in Nigeria with the attendant criminal activities on the internet necessitated an urgent need to formulate rules that will deal decisively with cybercrimes. The Cybercrimes Act was therefore enacted in 2015. The main purpose of the Act is to provide an effective, unified, and comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. The Act also ensures the protection of critical national information infrastructure and promotes cyber security and the

17 *Ibid*.
18 *Ibid*.
19 Telecommunications and Postal Offences Act 1995 but repealed in 2004 and 2016 respectively.
20 2006.

protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights.

i. Highlights of the Cybercrimes (Prohibition, Prevention, etc.) Act

The Act vests the power of apportioning and designation of certain computer systems and networks as critical national information infrastructure on the President of the Federal Republic of Nigeria, as well as the power of prescribing minimum standards for the handling of critical national information infrastructure, if recommended by the National Security Adviser to the President.[21] The president may delegate the exercise of these powers to the office of the National Security Adviser.[22] It is a criminal offence to access a computer that houses critical information infrastructure that is vital to national security. Such an act will render the person who commits the act liable to imprisonment for not more than 5 years or to an option of a fine of five million naira or both imprisonment and fine.[23]

It is also a criminal offence to have unlawful access to a computer with the intent to defraud other people.[24] A term of imprisonment of between 3-5 years and a fine ranging from seven to ten million awaits anybody who commits an offence under these sections. Equally, the Act finally criminalizes cybersquatting in Nigeria's cyberspace and this is a welcome development in the corporate world which suffers economic losses from the menace. Anybody found guilty of this offence will be liable on conviction to a term of imprisonment not exceeding 2 years or to a fine not more than five million or to both imprisonment and fine. Also, the Act criminalizes the negligent handling of personal data of citizens by service providers in Nigeria.[25] The Act provides individual and corporate penalties for contravention of the relevant provisions of the Act.

Furthermore, the Act provides for the regularity and binding effect of electronic signatures in respect of purchases of goods and other transactions.[26] However, the Act removes from its ambit the application of electronic signature to the following:

(a) creation and execution of Wills, Codicils, and or other testamentary documents;
(b) death certificate;
(c) birth certificate;
(d) matters of family law such as marriage, divorce, adoption, and other related issues;
(e) issuance of court orders, notices, and official court documents such as affidavits, pleadings, motions, and other related judicial documents and instruments;
(f) any cancellation or termination of utility services;
(g) any instrument required to accompany any transportation of dangerous materials either solid or liquid in nature; and
(h) any document ordering withdrawal of drugs, chemicals, and any other material either on the ground that such items are fake, dangerous to the people or the environment, or expired, by any authority empowered to issue orders for withdrawal of such items.[27]

Offences that were not originally designated as crimes under any known law in Nigeria were created by the Act and, individual and corporate liabilities and penalties such as committal of the directors of affected companies to various terms of imprisonment, as well as imposition of heavy

[21] Cybercrimes (Prohibition, Prevention etc.) s 3.
[22] S 4.
[23] S 6.
[24] Ss 13-15.
[25] Ss 25, 29 and 34.
[26] S 17 (1).
[27] S 17 (2).

fines on affected organizations were also created.[28] Business entities are mandated to report incidents amounting to cyber threats to the National Computer Emergency Response Team (CERT) Coordination Centre.[29] Service providers are to collaborate with law enforcement agents (including by providing access to data stored) concerning electronic transactions.[30] Institutions for the enhancement of cyber security are established.[31] Financial institutions are mandated to ascertain and secure the identities of customers who are provided with 'Access Devices' for computer transactions, and the duty of posting and authorizing access in a single employee is prohibited.[32] Sections 19, 20, and 37 impose a heavy burden on financial institutions to ensure that electronic banking and payments are secure. According to a learned author:

> Sections 19, 20, and 37 make financial institutions in Nigeria culpable. The culpability of financial institutions in Sections 19, 20, and 37 of the Act is a welcome development given the incessant ripping of innocent Nigerians of their hard-earned monies through spurious charges in the name of rendering 'seamless services' to them. The Act proactively superintends over the docility of the Nigerian Apex bank, the Central Bank of Nigeria in helping to sanitize its jurisdiction. Also, this section is a sword for any litigant in Nigeria whose identity has been stolen due to the negligence of any financial institution especially during the era of proliferation of private data like the Bank Verification Exercise.[33]

The Act makes provision for the payment of compensation and restitution to victims of cybercrimes. This is a landmark achievement because most criminal legislation only provides for the punishment of the offender without a corresponding restitution to the victims.[34]

The Federal High Court is vested with the jurisdiction to try all cybercrimes and provision is made for trans-border cooperation on investigation, prosecution, and enforcement of court judgments in respect of cybercrimes.[35] In the course of adjudication of disputes, the Federal High Court is not to entertain any stay of proceedings on any criminal matter concerning the Act. Thus, the Act recognizes the global nature of cybercrimes by designating the Federal High Court as the only court with exclusive jurisdiction to try cybercrimes. To forestall unnecessary delays in the adjudication of disputes, the Act prohibits the grant of a stay of proceedings in any cyber-related matter before the court. The Act mandates the office of the National Security Adviser to designate and maintain a contact point that will provide immediate assistance for international cooperation under the Act. The idea behind this initiative is to maintain a contact point where Nigeria can share important information on cyber security with other foreign countries.[36]

---

28 Ss 5-36, 46 and 58. The following were designated as cybercrimes under the Act: unlawful access to a computer system for fraudulent purposes, trafficking of passwords or similar information without lawful authority, interfering with computer systems which hinders the functioning of the computer system, intercepting electronic messages, emails and electronic money transfers, willful misdirection of electronic messages, theft of Automated Teller Machines and Point of Sales Terminals, phishing, spamming and spreading of computer viruses, computer related forgery and fraud and the unauthorized modification of data held in any computer system or network, the use of computer systems for child pornography, cyber stalking, identity theft and impersonation, racism, cybersquatting and electronic card related fraud.

29 S 21.

30 Ss 38-40.

31 Ss 42 and 44.

32 Ss 19, 20 and 37.

33 T Ilori 'The Nigerian Cybercrimes Act 2015: Is It Uhuru Yet?' <https://www.lawyard.ng.> accessed 13 June 2023.

34 S 49.

35 Ss 50-52.

36 S 56.

It is clear from the above provisions that the core achievements of the Act are the recognition of electronic signatures as valid and binding, and the provision for the establishment of a Cybercrime and Cyber Advisory Council. The Council is given wide powers to create an enabling environment and provide recommendations on the issues relating to the prevention and combating of cybercrimes, and the promotion of cyber security. Equally, the Act confers exclusive jurisdiction on the Federal High Court to try cyber-related offences. Cybercriminals can now be prosecuted for cybercrimes in the Federal High Court. The Act also provides for trans-border cooperation on investigation, prosecution, and enforcement of court judgments in respect of cybercrimes. Thus, there is now a collaborative effort to fight cybercrime between our country and other countries. Commenting on this development, Banwo and Ighodalo had this to say:

> The lack of a specialized statutory regime governing cyber-related contractual agreements in the past had limited not only the volume of commercial deals concluded electronically but also the number of cases instituted for seeking redress in cases of breaches…Disputes shall now be given speedy trial without room for interlocutory applications for stay of proceedings. Again, the Cybercrimes Act provides for cross-jurisdictional cooperation. This will ensure that investigation of allegations of offences shall enjoy mutual assistance from foreign countries while accused persons, against whom prima facie cases are established, and convicted persons in respect of trans-border transactions; shall be liable to extradition. In effect, there will be a better guarantee of the sanctity of commercial contracts.[37]

Speaking on the achievements of the Cybercrimes Act, another writer posits that:

> The Nigerian Cybercrimes Act has been able to show with ample evidence its readiness to restore confidence in Nigerian cyberspace. The punitive nature of the Act has helped to show a low tolerance of cybercrime activities by the government. The Act may be said to have achieved a fair result in this regard. Also, the Act has been able to show its dedication to sanitization of the ICT sector in Nigeria to help boost its prospects in e-commerce… Most importantly, with new provisions proscribing nefarious cyber-activities to ensure cyber-security in Nigeria, it shows to an extent Nigeria's readiness for digitization in the global cyber-society where technological innovations are fast becoming the best means of achieving positive might.[38]

There is hope that the new legal regime will boost the confidence of individuals, firms, and companies to transact more businesses and render services online, without the fear of falling victim to identity theft, plagiarism, or copyright violation.[39] The establishment of institutions that are going to work together to enhance cyber security in the country should further boost confidence and ultimately increase the volume of e-commerce. The institution of the Cybercrimes Advisory Council, which is the policy think-tank for coordinating all research and policy issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria should equally be geared towards the enhancement of electronic transactions in Nigeria.[40]

Regulation of Electronic Contracts in South Africa

In the online environment, the Electronic Communications and Transactions Act (ECTA) [41] is the major legislation that regulates electronic transactions in South Africa. The law came into being

[37] Banwo & Ighodalo (n 2).
[38] Ilori (n 33).
[39] Banwo & Ighodalo (n 2).
[40] *Ibid*.
[41] 25 of 2002.

after many years of legal uncertainty. Up till the enactment of the Electronic Communications and Transactions Act (ECTA), no law in South Africa comprehensively provided for electronic transactions. That notwithstanding, the courts were willing and gave legal recognition to electronic communications before the enactment of the ECTA. This is seen in *Council for Scientific and Industrial Research v Fijen,*[42] wherein the court stated that an E-mail sent to a superior indicating one's intent to resign constituted a valid letter of resignation in the context of a written and signed document. Similarly in *Balzan v O'Hara and Others,*[43] Coleman J. held that a telegram could constitute written and signed authority within the meaning of written and signed, as contemplated in the Land Alienation Act.[44]

Even the Interpretation Act made allusions to the fact that electronic impulses satisfy the requirement of signed writing when it states that:

> In every law, expression relating to writing shall, unless the contrary intention appears, be construed as including references to typewriting, lithography, photography, and all other modes of representing or reproducing words in visible form.[45]

Both the UNCITRAL Model Law on E-Commerce[46] and the UNCITRAL Model Law on Electronic Signatures[47] were influential in the drafting and formed the basis for the ECTA. The ECTA is one of the many sources of law that impact electronic communications and transactions and, must not be read in isolation of relevant statutory and common law. It applies to any form of communication by e-mail, the internet, SMS, etc., except for possibly voice communications between two people.[48] The ECTA however excludes four different instances where an electronic writing or signature would not be valid.[49] The four excluded acts are; concluding an agreement for the alienation (disposal) of immovable property as provided for in the Alienation of Land Act,[50] concluding an agreement for a long-term of immovable property above 20 years as provided for in the Alienation of Land Act,[51] the execution of a bill of exchange as defined in the Bills of Exchange Act,[52] and the execution, retention and presentation of a will or codicil as defined in the Wills Act.[53]

Apart from the ECTA, other legislation may apply to electronic contracts. They include the Interception and Monitoring Act,[54] Regulation of Interception of Communications and Provisions of Communication Related Act (RICPCRA),[55] the National Credit Act[56] (which has now repealed the old Credit Agreements Act, Act 75 of 1980).

---

42 (1995) ZASCA 143 (1996) (2) SA 1 (SCA), quoted in S Snail, 'Electronic Contracts in South Africa: A Comparative Analysis' [2008] (2) *Journal of Information, Law & Technology (JILT)* <https://www.warwick .ac.uk.>accessed 17 June 2023.

43 1964 (3) SA (T) 1.

44 LAA 68 of 1957.

45 Interpretation Act 33 of 1957.

46 UNCITRAL Model Law on Electronic (n 3).

47 See UNCITRAL Model Law on Electronic Signature 2001 adopted in 2001 General Assembly Resolution 56/80 of 5 July 2001 <https:// www.uncitral.org.> accessed 20 June 2023.

48 See Michalsons, 'Guide to the ECT Act in South Africa' <https:// www.michalsons.com.>assessed 18 July 2023.

49 ECTA s 4 (3) (4).

50 Alienation of Land Act 68 of 1981.

51 *Ibid.*

52 Bills of Exchange Act 7 of 1953.

53 Wills Act 34 of 1964.

54 Interception and Monitoring Act127 of 1992.

55 RICPCRA 70 of 2002.

56 National Credit Act 34 of 2005.

The ECTA has now entrenched the position that digitally negotiated and electronically signed contracts are fully valid and enforceable under South African law.[57]The ECTA Act provides for the legal recognition of data messages and the requirements of writing, signature, and contract formation. Section 12 of the ECTA recognizes data as the functional equivalent of writing or evidence in writing. It provides:

> A requirement under law that a document or information be in writing is met if, the document or information is:
> (a) in the form of a data message; and
> (b) accessible in a manner usable for subsequent reference.[58]

This section follows Article 6 of the UNICITRAL Model Law on E-Commerce as well as Article 9 (1) & (2) of the United Nations Convention on the use of Electronic Communications in International Contracts,[59] by guaranteeing data messages the same legal validity equal to messages written on paper. Article. 6 of the UNICITRAL Model Law on E-Commerce provides that:

> Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.[60]

Article 9(1) & (2) of the United Nations Convention on the Use of Electronic Communications in International Contracts similarly provide that:

> (1) Nothing in this convention requires communication or a contract to be made or evidenced in any particular form;
> (2) Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication, if the information contained therein is accessible so as to be usable for subsequent reference.[61]

Section 11(1) of the ECTA recognizes electronic data messages as a valid method of entering into electronic contracts and cannot be invalid due to their immaterial nature. The said section provides:

> (1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message;
> (2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.[62]

Section 11(1) of the ECTA follows Articles 4 and 11 of the UNCITRAL Model Law on Electronic Commerce, as well as Article 8 (1) of the United Nations Convention on the Use of Electronic Communications in International Contracts. Article 4(1) and (2) read together with Article 11(1) provides:

> As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided … the provisions of may be varied by agreement … it does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.' and 'In the context of contract formation, unless otherwise agreed by the parties, an offer and the

---

57 Snail (n 121).
58 Sec.12 ECTA.
59 United Nations Convention on the use of Electronic Communications in International Contracts 2005 adopted in 2005 by General Assembly Resolution A/60/21 <https:// www.uncitral.org.> accessed 20 June 2023.
60 UNCITRAL Model Law on E-Commerce 1996 art 6.
61 UNCECIC Art 9 (1) (2).
62 ECTA s 11(1).

> acceptance of an offer may be expressed using 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. [63]

Article 8(1) of the United Nations Convention on the Use of Electronic Communications in International Contracts[64] provides that a communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.

Section 4 (2) (a) & (b) of the ECTA makes it optional for any person who wants to use electronic communications for entering into a contract. It provides that:

> This Act must not be construed as requiring any person to generate, communicate, produce, process, send, receive, record, retain, store, or display any information, document, or signature by or in electronic form, or prohibiting a person from establishing requirements in respect of how that person will accept data messages.[65]

This provision is on all fours with Article 8 (2) of the United Nations Convention on the Use of Electronic Communications in International Contracts, which indicates that the use of electronic data messages is not mandatory but, may be done by choice or tacit consent based on the conduct of the contracting parties.

On the issue of the validity of electronic signatures in South Africa, Section 13 of the ECTA provides that a signature that was created using an electronic data message is valid. It similarly follows Article 7 (1), (2), and (3) of the UNICITRAL Model Law on E-Commerce as well as Article 9 (3) of the United Nations Convention on the Use of Electronic Communications in International Contracts, which ensure that data messages can satisfy the signature requirement. According to section 13 of the ECTA:

1. Where the signature of a person is required by law, that requirement in relation to a data message is met, if only an advanced electronic signature is used;
2. Subject to subsection (1) an electronic data message is not without legal force and effect merely on the grounds that it is in electronic form
3. Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if:
   (i) a method is used to identify the person and indicate the person's approval of the information contained; and
   (ii) having regard to all relevant circumstances at the time the method was used; the method was as reliable as was appropriate for the purposes for which the information was communicated.[66]

This section particularly follows Article 9(3) of the United Nations Convention on the Use of Electronic Communications in International Contracts, which ensures that data messages can satisfy the signature requirement. It provides:

> Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:
>
> (a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and

63 Art 4 (1) and 11(1) Model Law on E-commerce.
64 UNCECIC Art 8(1).
65 ECTA s 4 (2) (a) (b).
66 ECTA s 13.

(b) The method used is either:
   (i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
   (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.[67]

As for the time of conclusion of the electronic contract, section 22 (2) of the ECTA provides that contracts concluded using data messages are concluded at the time, and the place where the acceptance of the offer was received by the offeror. In other words, the ECT Act adopted the reception theory for electronic contract formation. This specifically marks the ECTA out from other countries' legislation, in the sense that the ECTA is the only legislation that makes specific provisions for the time an electronic contract is concluded. According to Pistorius,[68] the ECT Act provides clear rules for the time and place that the dispatch and receipt of data messages become effective. The ECT Act makes specific provisions for the time an electronic contract is concluded. This salient feature of the ECT Act is in stark contrast to the uncertain legal position obtained in other jurisdictions.[69]

The ECTA is therefore an all-encompassing legislation, and that makes it unique, unlike most electronic transaction legislation. Apart from the fact that it contains provisions providing for the recognition of data messages as a means of entering into contracts, and guarantees functional equivalence between paper-based and technology transactions, it equally provides for the protection of consumers and private data as well as cybercrimes. For instance, section 43[70] provides that suppliers of goods or services must provide consumers with a minimum set of information, including the price of the product or service, the name, contact details, a brief description of the business, and the right to withdraw from an electronic transaction before its completion. Consumers are also entitled, under certain circumstances, to a 'cooling off' period within which they may cancel certain types of transactions concluded electronically without incurring any penalty.[71] Consumers also have the right not to be bound to unsolicited communications (spam) offering goods or services, and the sender of the unsolicited communication must at the request of the consumer, provide the identifying particulars of the source from which it obtained the consumer's personal information.[72] A person who continues to send unsolicited communications to a consumer after having been advised that the unsolicited communications are not welcome, commits an offence.

The ECT Act also seeks to place the responsibility on businesses trading online to make use of sufficiently secure payment systems. If a payment system is breached as a result of the system not being sufficiently secure, the supplier must reimburse the consumer for any loss suffered.[73] Equally, the Act establishes a voluntary regime for the protection of personal information. Collectors of personal information (data collectors) may subscribe to a set of universally accepted data protection principles.[74]

---

67 UNCECIC Art 9 (3).
68 T Pistorius, 'Formation of Internet Contracts: Contractual and Security Issues' [1999] (11) *SA Mercantile Law Journal*, 281-286.
69 *Ibid*.
70 ECTA.
71 ECTA s 44.
72 *Ibid* s 45.
73 S 43 (5) (6).
74 S 50.

Lessons for Nigeria

There can be no doubt that the stage for electronic contracts is set in Nigeria. This is made manifest in the number of efforts made at legislating for electronic contracts in the country and, the volume of internet contracts presently undertaken by her citizens. As captured by Kazeem:

> There have been several legislative strides made since the early days of internet commerce and in Europe and America, there has been an almost frenzied approach to removal of legal bottlenecks against this recognition and enforcement of E-contracts. In Nigeria, while the pace may not be as frenetic, it is gathering steam.[75]

It is unarguable that, not much has been done in Nigeria regarding the regulation of electronic contracts when compared to South Africa. South Africa enacted legislation that tackles all electronic transactions without narrowing it to electronic contracts. Most importantly it made a definitive pronouncement on when an electronic contract will be deemed to have come into existence. Although Nigeria curled the Electronic Transactions Bill from the South African ECTA, no serious effort is being made to pass the Bill into law. What we have in Nigeria so far is the stretching of existing laws to new and flexible technology which is not likely to give electronic contracts the desired legal status and protection. If our neigbours can do it, then Nigeria can equally follow their footprints and enact comprehensive legislation that will cater for electronic contracts. To this end, our preoccupation should be on enacting legislation that is both functionally equivalent and technologically neutral. It is a heartwarming development that our Electronic Transactions Bill is a replica of the Electronic Communications Transaction Act of South Africa.[76] The said Act has been adjudged one of the best in the world as far as electronic transactions are concerned. Apart from providing for the legal recognition of online contracts, admissibility of electronic documents, data protection, protection of consumers of online goods and services as well as the provision of mechanisms for checking cybercrimes, it is the first legislation to provide for the exact moment an electronic contract would be deemed to have come into existence.

It is urged that the shortcomings identified in the Electronic Transactions Bill should be addressed and the Bill amended to reflect those changes. Once this has been done, the president should without further delay assent to the Bill. With a good legal landscape for electronic contracts and other electronic transactions, Nigeria will be seen by the international community as a good place to do business and even, as a choice of law and jurisdiction for electronic contracts.

Conclusion

The above discourse has demonstrated that Nigeria is lagging in terms of enjoying the benefits of technological advancements. It is clear that if Nigeria wants to enjoy all the benefits attendant with electronic transactions, she needs to up her game and enact comprehensive legislation that will regulate electronic contracts like that of South Africa which has been adjudged one of the best in the world. The uncertainty surrounding cyberspace in Nigeria would not have been there if there had been comprehensive legislation in place to cater to electronic activities. The Electronic Transactions Bill is long overdue for passage into law. Nigeria should pride herself in place of the committee of nations with vibrant legislation to cater to the ever-evolving cyber technology. A law that will stand the test of time is a necessity for Nigeria.

---

[75] MA Kazeem, 'Electronic Contract Formation and the Nigerian Initiatives' <https://www.academia.edu accessed 18 June 2023.

[76] ECTA 25 of 2002.