Legal Frameworks for the Implementation of Electronic Governance in Nigeria and Matters Arising

[1*]Okeji S.M., [2]Adedoyin-Raji J.O. & [2]Isa Y.I.
[1]Registry Department, Federal University of Technology, Minna
[2]Nasarawa State University, Keffi
[*]Corresponding author: smokeji@futminna.edu.ng

Received: 22/07/2024 **Revised: 20/09/2024** **Accepted: 13/11/2024**

The increasing use of the Internet has accelerated this widening of the scope of privacy to the protection of private information as well. The exponential growth of electronic usage in global transactions has created new challenges to existing laws. Some of the legal solutions still lag, because of the unique complexities attached to e-activities. Electronic evidence is subject to the same evidentiary rigours as its paper –based counterpart. Electronic evidence as with other evidence, must be both material and relevant to the issues as defined by pleadings, must not be subject to any other exclusionary rule and must be ultimately possess greater probative value than prejudicial effect to be received. There exists no legislation on electronic signature in Nigeria which is vital for authentication of electronic evidence or digital evidence to determine its genuineness and reliability. The paper examined the implementation of electronic governance in Nigeria thus the issues arising therefrom towards an improved e-governance system. The paper relied on doctrinal analytical method of research by which primary sources of enabling legislations were consulted and relevant secondary materials /treaties for ease of comparison. There exists inadequate legislation that will boost the confidence of the citizenry on implementation and integrity of the system because of these inadequacies. It is in this light the paper concludes that tackling the obstacles to e-governance adoption is key to the citizen centric quality service delivery. The paper recommends a strengthened and gazette critical information infrastructure, enactment of digital signature law, forensic/digital laboratory, and establishment of National Data bank.

Keywords: Electronic Governance, Critical information infrastructure, Cybercrimes, Digital Forensic, Electronic signature, Technology Acceptance Model

https://dx.doi.org/10.4314/etsj.v15i2.16

Introduction

The development of technological tools and the changes in citizens' profiles, e-government is evolving to Digital Governance (d-governance)[1]. It goes beyond electronic services provided, citizens can participate in decision-making processes through online interactions. Digital Governance is promoted by greater transparency and by citizen participation through online tools, developed by both government and society.

The use of information and communication technology (ICT) which currently dominated our daily lives and economic interactions has led to an increase in cybercrimes in the forms of hacking, infringement of intellectual property, credit card theft, phishing, spamming, cyber stalking, cyber-squatting, illegal access to data, misuse of computer devices for fraud, cyber terrorism and other forms of online crimes[2] system interference,[3] computer related fraud and forgery,[4] misuse of devices for crime,[5] illegal interception,[6] intellectual property violations, terrorism and viral attacks[7]. Any crime committed in the cyberspace is a cybercrime; or put in a more succinct way, any crime committed by using computer as a tool for the perpetration of the offence can generally be described as a cybercrime. Such act includes hacking, cracking, stalking, squatting, phishing, identity theft, impersonation, spoofing, software piracy, credit card fraud and viral attacks through the use o computers[8].

Cybercrimes threat is not limited to Nigeria but a global phenomenon beyond compromise but due to sophistication. Cybercrime report in 2021 in the United States of America, United Kingdom, and Australia showed that a number of agencies like the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency, National Security Agency and Cyber Security Centre in 2021[9], detected an

[1]S. Greenberg and A. Newell. Transparency Issues in E-Governance and Civic Engagement. In Active Citizen Participation in E-Government (2012)pp.44-64. IGI Global. <https://doi.org>accessed on 25 April 2024.

[2]Olanrewaju Adesola Onadeko and Abraham Femi Afolayan, A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria. Being a paper presented at the 29th International Conference of the International Society for the Reform of Criminal Law (ISRCL) held at Halifax, Nova Scotia, Canada July 24 – 28, 2016.

[3] CA S.8

[4] CA S.14

[5] CA s16

[6] CA s12

[7] CA s18

[8]Olanrewaju Adesola onadeko and Abraham Femi Afolayan, A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria. Being a paper presented at the 29th International Conference of the International Society for the Reform of Criminal Law (ISRCL) held at Halifax, Nova Scotia, Canada July 24 – 28,(2016).

[9] James Chike Nwankwo, Cyber-Security in Nigeria. *A Case Study of Surveillance and Prevention of Digital Crime by*

increase in cyber-attack sophistication in infrastructure. The challenge of Cybercrime is more prevalent in West African countries. Internet users in Ghana reached approximately 17 million, as of January 2022, which statistics shows 53% of the Ghana population[10] but Nigeria is one country mostly affected by cybercrime[11] cybercriminals which had severe influence on finances, reputation, and growth of the region.[12]

Most orchestrated cybercrimes originated locally from Nigeria, but it is noteworthy that these malicious activities involve collaborations with nationals from other countries, such as South Africa and Cameroon[13]. Nigeria is one of the countries mostly affected by cybercrime, according to recent studies[14]. Cybercriminals have been able to target people and businesses in Nigeria based on the expansion of digital technology and internet usage, which had severe influence on finances, reputation, and growth of the region[15]. In the 2000s, there was an upsurge in imitations of email scams emerging from various locations in Africa, Asia, and Eastern Europe, which indicates that local elements heavily influence the cybercrime landscape in Nigeria but also have a significant international dimension. Ransom ware attacks on Nigerian businesses skyrocketed from 22% in 2020 to 71% in 2021, with affected companies paying an average of $3.43 million compared to $0.46 million in the previous year. External threats are evident with entities like ”Anonymous” allegedly targeting major financial infrastructures such as the Central Bank of Nigeria in 2020[16] These cyber vulnerabilities, both domestic and foreign, have not only paralyzed 97% of affected businesses but also resulted in significant revenue losses for 96% of them[17]. Furthermore, because hackers now operate across borders and jurisdictions, it is challenging for law enforcement organizations to investigate and prosecute cybercrime crimes.

The increasing use of the Internet has accelerated this widening of the scope of privacy to the protection of private information as well. The exponential growth of electronic usage in global transactions has created new challenges to existing laws. Some of the legal solutions still lag, because of the unique complexities[18] attached to e-activities. Electronic evidence is subject to the same evidentiary rigours as its paper –based counter-part[19]. Electronic evidence as with other evidence, must be both material and relevant to the issues as defined by pleadings, must not be subject to any other exclusionary rule and must be ultimately possess greater probative value than prejudicial effect to be received[20].

There exists no legislation on electronic signature in Nigeria which is vital for authentication of electronic evidence or digital evidence to determine its genuineness and reliability. However, the Act in its definition of electronic evidence as a document to include any device used for storing, recording, or retrieving information, including computer output[21]and evidence that is generated through mechanical or electronic processes[22]. It involves the use of electronically controlled machines or equipment, such as computers, satellite waves, cables, and communication systems, to gather evidence for use in a court of law. The lack of researches relating to the barriers in electronic/Digital Governance adoption in Nigeria and the absence of legal framework for the adoption of secured e-governance in Nigeria outside the legislation and the initiatives in silos were the main reasons that drive this study. Therefore, the research questions are

How is cybercrime a major barrier for digital governance adoption in Nigeria?

Are there legal frameworks that can be assessed for the implementation of electronic governance in Nigeria?

Lorliam. A Review beyond Mere Digital Surveillance: Journal of Artificial Intelligence & Cloud Computing (*Arti Inte & Cloud Comp, 2022) Volume 1(3): 1-4*

[10] Digital 2022: Nigeria — DataReportal – Global Digital Insights <https://datareportal.com/reports/digital-2022-nigeria>accessed on 9 September 2024

[11]F. A. Duah and A. M. Kwabena, “The impact of cybercrime on the development of electronic business in Ghana,” European Journal of Business and social sciences, vol. 4, no. 1, pp. 22–34, 2015.

[12]O. Longe and others, “Criminal uses of information & communication technologies in sub-saharan africa: Trends, concerns and perspectives,” Journal of Information Technology Impact, vol. 9, no. 3, pp. 155–172, 2020.

[13] O. Longe and Others Ibid- 2020

[14]F. A. Duah and A. M. Kwabena, “The impact of cybercrime on the development of electronic business in Ghana,” European Journal of Business and social sciences, vol. 4, no. 1, pp. 22–34, 2015.

[15]O. Longe, and Others, “Criminal uses of information & communication technologies in sub-saharan africa: Trends, concerns and perspectives,” Journal of Information Technology Impact, vol. 9, no. 3, pp. 155–172, 2009.

[16]B. Ikusika, “A critical analysis of cybersecurity in Nigeria and the incidents of cyber-attacks on businesses/companies,” Companies (July 15, 2022), 2022.

[17]O. Ede and G. Okafor, “The impact of kidnapping on foreign ownership of firms in Nigeria,” Thunderbird international business review, vol. 65, no. 3, pp. 341–354, 2023.

[18]B. Schafer and S. Mason, The characteristics of Electronic evidence in S.Mason and Seng (ed) Electronic Evidence (2017)page 19 cited in Alaba Omolaye Ajileye,Electronic evidence, Jurist Publication Series, Lokoja, Nigeria, 2019 Rev. edn P.74.

[19]Abdulsalam O. Ajetunmobi, Information and Communications Technology Law in Nigeria, A Comparative Reader: Princeton and Associates Publishing co ltd (2017) p.118.

[20]Karen Groulx and Chuck Rothman: Electronic Evidence Admissibility: Understanding Types and Sources of Electronic Evidence, Karen Kroulx, Dentons Canada (2011) p.22.

[21]Evidence Act, 2011 S.58(1)d.

[22]P. A. Anyede, ‘Appraisal of Admissibility of Electronic Evidence in Legal Proceedings in Nigeria’ (2019) 29 Journal of Law, Policy and Globalization,3.

Literature Review

The term governance was coined from the Latin word "gubertnare" and originate from the Greek word "Kubernaein that means to steer[23] Governance indicates to steer, direct or control a state or group of people and covers the areas of structures, processes, which are devised to ensure transparency, responsibility receptiveness, rule of law, consistency, equality, liberation, and general participation[24].

Governance also includes the standards, moral and principles through which public matters are resolved in an impartial way[25]**.** Thus, in a broad sense it can be said that governance is about the culture and the established environment where people with different interests interact in various public affairs. Therefore, it is something subtle and may not be clearly noticeable. It can be considered as the most vital organ of the government!

Electronic Governance (e-Governance) is the application of information and communication technology (ICT) for delivering government services, exchange of information,[26] transaction, running of government administration involving the state, non-state actors, businesses and the citizenry ensuring an inclusive and participatory governance. E-Governance involves the use of Information Technology, especially the Internet, to promote the delivery of government services to citizens, businesses and society. This allows for greater interaction of actors with state agencies, twenty-four hours a day, seven days a week[27]. The focus of Electronic Government efforts is to deliver services more efficiently and effectively[28] attenuating the excessive dependence on the government intermediation between services and citizens[29]. The globalized world now exposes individuals to all manner of vulnerability that is not constrained by the usual barriers of physical distance. Indeed, even if one does not use the Internet, much of his/her personal information is possibly stored somewhere on a networked computer**[30].** By all means, every individual is a potential victim of cybercrime[31]. The above implication is that cybercrime victimization is now a global social problem: defying several mitigating measures. Internet-enabled crimes and scams have shown no sign of letting up[32]. This development has also changed the role of the government in guaranteeing privacy[9] Developments in privacy issues have also given rise to government obligations to actively guarantee the right to a private life and to prevent invasion, not only by government agencies themselves but also by third parties[33].

Committed by using computer as a tool for the perpetration of the offence can generally be described as a cybercrime. Such act includes hacking, cracking, stalking, squatting, phishing, identity theft, impersonation, spoofing, software piracy, credit card fraud and viral attacks through the use o computers[34]. The global nature of the internet makes it easy for criminals armed with a computer and the internet to victimize individuals and businesses anywhere in the world right inside his home[35]**.**

[23]Plattner, 2013 cited in Ridoan Karim, Tasmeem Chowdhury Bonhi, Rawnak Afroze Governance Of Cyberspace: Personal Liberty VS. National Security international journal of scientific & technology research volume 8, issue 11, november 2019 issn 2277-8616 2636 ijstr©2019<https:// www.ijstr.orgaccessed> on 11 July 2024..

[24]Ridoan Karim, Tasmeem Chowdhury Bonhi, Rawnak Afroze, Governance Of Cyberspace: Personal Liberty VS. National Security international journal of scientific & technology research volume 8, issue 11, november 2019 issn 2277-8616 2636 ijstr©2019 <www.ijstr.org>accessed on 30 June 2

[25]Franz Nuscheler, & Veronnica Wittmann, From governance to good governance.Sustainable Development Policy: A European Perspective, 91(2017) cited in Ridoan Karim, Tasmeem Chowdhury Bonhi, Rawnak Afroze, Governance Of Cyberspace: Personal Liberty VS. National Security international journal of scientific & technology research volume 8, issue 11, november 2019 issn 2277-8616 2636 ijstr©2019 <www.ijstr.org>accessed on 30 June 2024.

[26]D. Infanta Michael Jenifer and M. Deepamalar, Anti-Cybercrime Technologies For E-Governance, International Journal of Innovative Research in Science, Engineering andTechnology,(IJIRSET)2017vol.6issue 5<www.ijirset.com>accessed 28 July 2024

[27]S.Nawafleh, R.Obiedat, & O.Harfoushi, E-Government between developed and developing countries. International Journal of Advanced Corporate Learning (iJAC),5(1),(2012) 1–12<https://doi.org>.

S. Greenberg and A. Newell. Transparency Issues in E-Governance and Civic Engagement. In Active Citizen Participation in E-Government (2012)pp.44-64. IGI Global. <https://doi.org>accessed on 25 April 2024.

[28]S. Greenberg and A Newell. Transparency Issues in E-Governance and Civic Engagement. In Active Citizen Participation in E-Government (2012)pp.44-64. IGI Global. <https://doi.org>accessed on 25 April 2024.

[29]R.Tassabehji, R Hackney and A Popovič, Emergent digital era governance: Enactingthe role of the 'institutional entrepreneur' in transformational change. Government InformationQuarterly, (2016) 33(2), 223– 236. <https://doi.org >accessed on 15 May 2024.

[30]M. Yar, The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology,* (2005 *2*(4), 407-427<http://www.cybercrimejournal.com>.accessed on 14 July 2024

O. F. Nzeakor, B N Nwokeoma and P J Ezeh Pattern of cybercrime awareness in Imo State, Nigeria: An empirical assessment. *International Journal for Cyber criminology*, (2020) *Volume 14, Issue 1,* January- June. <http://www.cybercrimejournal.com>.accessed on 14 July 2024.

[32]N. Ndubueze, (Ed.). *Cyber criminology and technology-assisted crime control:* Ahmadu Bello University Press Limited Wall, (2017) P.360.

[33]O F.Nzeakor, B N Nwokeoma, and J T Okpa, Emerging Trends in Cybercrime Awareness in Nigeria. International Journal of Cybersecurity Intelligence & Cybercrime: (2022) 5(3),41-67< https://doi.org>accessed on 11 july 2024

[34]Olanrewaju Adesola onadeko and Abraham Femi Afolayan, A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria. Being a paper presented at the 29th International Conference of the International Society for the Reform of Criminal Law (ISRCL) held at Halifax, Nova Scotia, Canada July 24 – 28 (2016).

[35]Bolaji Owasanoye, "Information Technology and Criminal Justice Administration" (2010) NLRJ 13 at 20).

Theoretical Framework Underpinning the Study

The appropriate theories for this study are innovation adoption theories. The use of information and communication technologies brought about far reaching benefits, convenience, improved performance, transparency, financial and time efficiency. The potential of technology to deliver benefits has long motivated Information Science (IS) management research to examine the willingness of individuals to accept innovative technology[36]. Over the years**,** research has focused on innovations that can be selected and technology[37]adopted which has resulted into various terms used in the studies, such as information and communication technology (ICT), Information Technology (IT), Information System (IS). These are not exhaustive and are interchangeable in use. The deployment of adoption of technology in research became of primary importance in the 1980s, which coincided with the growth of the use personal computers[38]**.** The study underwent several investigations which culminated in IS, IT research theory models for usability, adoptability and behavioural approach and acceptance. This makes the theory acceptable for this study. Advancement in the theory brought about Diffusion of Innovation (DOI) theory, Technology Acceptance Model (TAM), and Theory of Reasoned Action (TRA) developed by E.M. Rogers in 1962[39]. Research from various disciplines has used the model as a framework especially in economics, political science, health, technology, communication and Rogers' theory as a widely used theoretical framework in the area of technology diffusion and adoption[40]. For Rogers, "a technology is a design for instrumental action that reduces the uncertainty in the cause-effect relationships involved in achieving a desired outcome". It is composed of two parts: hardware and software. While hardware is "the tool that embodies the technology in the form of a material or physical object," software is "the information base for the tool"[41]. Since software (as a technological innovation) has a low-level observability; its rate of adoption is quite slow[42].The behaviour of an individual, belief, attitude of the mind and expected reward all work together[43]. Davis developed the model of technology acceptance by framing the processes mediating the relationship between IS characteristics (external factors) and actual system use[44]. TAM describes the two constructs of external factors (such as technology, people and process) determines the perceived usefulness and the perceived ease of use. Although TAM theory is robust and ease with use because of its acceptance behaviourally on IS application and its motivating less labour intensive, researchers have identified vulnerability in it. In terms of theoretical foundations, these studies focus on the adoption of these best practices and lean heavily on the adoption of technology literature[45].

The theory is applicable to the practice of e-governance in the Nigerian. Technology Acceptance Model is relevant to the Nigerian as it explains the role played by self-efficacy, perceived cost, technological infrastructure, power supply, and internet facilities to support the adoption of e-governance. The application of TAM is enhanced due to its simplicity together with the predictive authority which makes its application easy to different situations[46]. Technology Acceptance Model is useful in explaining the acceptance, application, relevance and effectiveness of modern technologies in information sharing among citizens, literacy level and galvanizes public service delivery. The application of TAM to a study like this underscores user's technological behaviour and actual utilization. From the analysis and with the assumptions of the TAM, the model is relevant and applicable to the discussion of e-governance implementation[47] and public service delivery in Nigeria. The theory is quite relevant and useful to policy makers, management of organizations and personnel in the selection of novel technical

[36]F. D. David. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. (1989)*MIS Quarterly*, 13 (3), 319.

[37]F .D. David Ibid p.319.

[38]Davit Marikya and S.Papagiannidis, Technology Acceptance Model: A review.In S.Papagiannidis(Ed), TheoryHub Book.2023<https://open.ncl.ac.uk> accessed on 28 February 2024.

[39]Everett M.Rogers,Diffusion of Innovation, 5th 2003 New York Press,p.551 <hhttps://sphweb.bumc.bu.edu.behavioralchangetheories4>accessed on 28 February 2024.

[40]Ismail Sahin, Detailed Review of Rogers' Diffusion of Innovations Theory and Eductional Technology related studies based on on Rogers' theory, Turkish Online Journal of Educational Technology (TOJET) 2006 vol.5 issue 2< https://eric.edu.gov> accessed 4 March 2024.

[41]Everett M.Rogers, Diffusion of Innovation, 5th 2003 New York Press,p.13 <hhttps://sphweb.bumc.bu.edu.behavioralchangetheories4>Rogers, 2003, p. 259.

[42]Everett M.Rogers Ibid p.266.

[43]I Ajzen, Attitudes, traits, and actions: Dispositional prediction of behavior in personality and social psychology. In L Berkowitz (Ed.), *Advances in experimental social psychology* ((1987) Vol. 20, pp. 1-63). New York: Academic Press.

[44]F. D. Davis. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quartely, 13(3), 319

[45]S Dawes,The Evolution and Continuing Challenges of E-Governance, Public Administration Review68(8) (2008), 82-102.

[46]Abasiama Godwin Akpan and David Aniefiok Titus, Assessing E-Governance Implementation in Nigeria Through the Technology Acceptance Model (tam) Application GSJ: Vol. 7, Issue 5 www.globalscientificjournal.comaccessed on 16 September 2024

[47] Abasiama Godwin Akpan and David Aniefiok Titus Ibid p.246

innovations and applications such as electronic governance[48].

Research Methodology

Doctrinal analytical research method is adopted in this study. A major reliance was placed on gathering the relevant information from the Constitution, Cybercrimes Act, Data Privacy Act, Evidence Act, Administration of Criminal Justice Act as a primary source of data and other enactments. Secondary sources of data were consulted from reported cases, laws from other jurisdictions, Treaties, Textbooks, scholarly journals, Commissioned papers, Circulars, reports, research thesis, newspapers and conference papers.

Matters Arising

The Constitution[49] guaranteed "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications and protected"[50] "and every individual is entitled to respect for the dignity of his person"[51] The constitution did not give an "interpretation or the meaning to the concept of privacy right that is guaranteed"[52]. The National Information Technology Development Agency (NITDA) is the authority responsible for planning, developing and promoting the use of information technology in Nigeria[53]

The exponential growth of electronic usage in global transactions has created new challenges to existing laws. Some of the legal solutions still lag, because of the unique complexities[54] attached to e-activities.

Electronic evidence is subject to the same evidentiary rigours as its paper –based counter-part[55]. Electronic evidence as with other evidence, must be both material and relevant to the issues as defined by pleadings, must not be subject to any other exclusionary rule and must be ultimately possess greater probative value than prejudicial effect to be received[56].

There exists no legislation on electronic signature which is vital for authentication of electronic evidence or digital evidence to determine its genuine and reliability. However, the Act in its definition of electronic evidence as a document to include any device used for storing, recording, or retrieving information, including computer output[57]and evidence that is generated through mechanical or electronic processes[58]. It involves the use of electronically controlled machines or equipment, such as computers, satellite waves, cables, and communication systems, to gather evidence for use in a court of law. This type of evidence can be obtained from various sources, including emails, phone logs, ATM and POS transaction logs, social media records (such as Facebook, Twitter, WhatsApp, Instagram), videos on platforms like YouTube, and digital content stored in DVDs, CDs, and flash drives[59]. In the case of Orogun & Anor v. Fidelity Bank[60] the Supreme Court addressed the admissibility of electronically generated evidence, specifically pertaining to a GSM gadget and the information stored within it. The court referred Section 258 (1)(d) of the Evidence Act, which defines a document to include any device used for storing, recording, or retrieving information, including computer output and admitted it in evidence. A party seeking to tender a computer-generated statement or document is required to file an authentication certificate. This certificate must identify the document or statement, describe the manner of its production, state the particulars of the device used, and be signed by a person in a responsible position in relation to the operation of the device or the management of the activities. The authentication certificate is a legal requirement aimed at ensuring the authenticity of electronic evidence before it can be admitted[61]. This position of authentication is yet to be settled on electronic evidence consideration case of Brila Energy ltd V. FRN, held that " a Court is permitted by law to admit in evidence records said to have been meticulously kept in the course of the business of a company and the issues relating thereto are brought before the court on enquiry"[62] The Court of Appeal did not accede to the objection for its admissibility because of lack of authentication and held that authenticity may be dispensed with when tendering

[48]Marco Yzer, Reasoned Action Theory, Persuation as Belief based Behaviour Change. Sage Publications Inc. 2013 <S3.amazonaws.com> accessed on 4 March 2024.
[49]Constitution Federal Republic of Nigeria (CFRN) (1999) as amended
[50]CFRN Ibid S.37
[51]CFRN Ibid S.37
[52]Iheanyi Samuel Nwankwo, Information Privacy in Nigeria, Institute for Legal informatics, Leibniz Universitat, Hannover, Germany,A.B. Makulilo (ed.), African Data Privacy Laws, Law, Governance and Technology Series 33, Springer International Publishing AG 2016 P.47.
[53]National Information Technology Development Agency (NITDA) Act 2007.
[54]B Schafer and S Mason, The characteristics of Electronic evidence in S.Mason and Seng (ed) Electronic Evidence (2017)page 19 cited in Alaba Omolaye Ajileye,Electronic evidence, Jurist Publication Series, Lokoja, Nigeria, 2019 Rev. edn p.74.
[55]Abdulsalam O Ajetunmobi, Information and Communications Technology Law in Nigeria, A Comparative Reader: Princeton and Associates Publishing co ltd (2017) p.118.
[56]Karen Groulx and Chuck Rothman: Electronic Evidence Admissibility: Understanding Types and Sources of Electronic Evidence, Karen Kroulx, Dentons Canada (2011)p.22.
[57]EAct, 2011 s58(1)d.
[58]P. A. Anyede, 'Appraisal of Admissibility of Electronic Evidence in Legal Proceedings in Nigeria' (2019) 29 Journal of Law, Policy and Globalization,3.
[59]Ibid.
[60]2018LPELR-46601(CA).
[61]Ayodeji v FRN (2018) 45839 (CA)4041.
[62](2018) LPELR-CA/L/658CA/2017@p.59.

a computer generated evidence . This area of our evidence of computer-generated evidence is yet to be finally settled[63].

Privacy and Security is one of the critical challenges of e-governance. Privacy, negatively stated, protects individuals against interference in their autonomy by governments and by private actors"[64] There "existed no single legislation in Nigeria that protect the data privacy of the citizen and foreigner"[65] before 12th June 2023"[66] which repealed the Nigeria Data Protection Regulation[67] that provided an "important framework to safeguard the rights of citizens to data privacy. It provides that no data shall be obtained except the specific purpose of the collection is made known to the data subject. It also mandates that the data collector obtains consent of the data subject before using this data[68]. This Act shall apply to the following persons, who shall be registerable persons in respect of whom entries shall be recorded in the Database, that is:

(a) any person who is a citizen of Nigeria;
(b) any person whether or not he is a citizen of Nigeria, who is lawfully and permanently resident in Nigeria; and
(c) any non-citizen who is lawfully resident in Nigeria for a period of two years or more[69]

These provisions could be dispensed with where the Security of the state is involved and also where court ordered.

Infrastructure is essentially required for implementation of e-governance in Nigeria. Electricity, internet and poor adaptability of technology will retard the Progress of e-governance. The Act empowered the President to "publish in the gazette, designate certain computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic, security,

National public health and safety, or any combination of those matters as constituting critical National Information Infrastructure[70] depending on the recommendation of the National Security Adviser. There should be an Act for implementation of e-governance Nigeria outside its operation in silos as Treasury Single Act (TSA), IPPIS, ATM operations being regulated by policy pronouncements[71] instead of statutory enactments.

Conclusion

Nigeria should strengthen its data security and ensures full implementation of the provisions of the Data and Privacy as enacted. The National Assembly should pass a bill for the entrenchment of electronic signature and for the establishment of National Data bank as has been done in other jurisdictions outside its reference in the Act[72]. This will instil trust and confidentiality on citizens and foreigners dealing with Nigerians on line. This measure will equally strengthen Courts pronouncement towards a uniform approach. Fundamentally, there should a national digital forensic laboratory where digital experts on electronic evidence can access metal data for real time analysis of genuine and reliable electronic data. The National Security Adviser should be emphatic on the designation of critical information infrastructure to be gazetted in compliance with the Cybercrimes Act. The Court[73] provided in the Data Privacy Act should be clear for enforcing the Act.

[63](2018) LPELR-CA/L/658CA/2017@p.59.
[64]De Hert p.&S.Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' E. Claes, A. Duff & S. Gutwirth. (eds..), Privacy and the criminal law, Antwerp/Oxford, Intersentia,2006.
[65]Iheanyi Samuel Nwankwo, Information Privacy in Nigeria, Institute for Legal informatics, Leibniz Universitat, Hannover, Germany, A.B. Makulilo (ed.), African Data Privacy Laws, Law, Governance and Technology Series 33, Springer International Publishing AG 2016 Page 47.
[66]Nigeria Data Protection Act, 2023 (NDPA) signed into law
[66]Iheanyi Samuel Nwankwo, Information Privacy in Nigeria, Institute for Legal informatics, Leibniz Universitat, by President Bola Ahmed Tinubu, GCFR on the 2th of June,2023..
[67]NDPR Implementation Framework was signed on 17th November 2020 by Director General, NITDA.
[68]NPDA ss 24,25 and 26
[69]National Identity Management Commission Act 2007 s.16.
[70]CA s3(a-c)
[71]Femi Daniel: Introduction to Computer Law in Nigeria, Ins-Spire Ventures Ltd, (2015) p.33.
[72]CA s17
[73]DPA s50