CYBERSTALKING AND ADMISSIBILITY OF ELECTRONIC EVIDENCE ON PUBLICATION OF NUDE PICTURE/VIDEO ON SOCIAL MEDIA: REVIEW OF *FEDERAL REPUBLIC OF NIGERIA V CHARLOTTE DEHLI**

Abstract
This review paper examines the controversy emanating from the interlocutory decision of the court in the Federal Republic of Nigeria v. Charlotte Dehli concerning a cyberstalking offence (publication of nude picture/video on social media). The court rejected the admissibility of a printout of a WhatsApp conversation from a mobile phone in evidence sought to be tendered by the prosecution in proof of its case. The court based its decision on the discrepancy concerning the testimony and the certificate tendered by the prosecution witness. However, this review paper argues that considering the current position of the law on issuance of certificate for authentication and what is obtainable in other jurisdictions, the court ought not to have relied on a technical or procedural error to reject the electronic evidence, which works against the interest of justice, instead, admit the same in evidence and determine the weight to be attached.

Keywords: Cyberstalking, Nude Pictures and Videos, Social Media, WhatsApp, Electronic Evidence, Cybercrime Law

1. Facts

The defendant who had sexual intercourse with one Dr Walton Liverpool in a Hotel room on 14 September 2021 was alleged to have video-recorded the incident without the consent of Dr Liverpool (a former permanent secretary of the Bayelsa State Ministry of Education). She later requested the sum of about N15, 000,000.00(Fifteen Million Naira) from Dr Liverpool as a kind of blackmail to prevent her from sharing the same on social media, which he could not afford. Consequently, the defendant shared the video on social media-a WhatsApp group tagged 'off Liverpool' with an Iphone 7 plus mobile phone and GSM No 08084267342. She is currently standing trial, having been arraigned by the Department of State Security Services (DSS) before the Federal High Court, Yenagoa, for cyberstalking contrary to section 24(2)(c) of the Nigerian Cybercrimes Act 2015. On 21 October 2021, in the course of the proceedings in proof of the prosecution's case, the prosecution sought to tender a printout of a WhatsApp conversation from the mobile phone of PW1(Dr Liverpool) in evidence. The conversation was purported to be held between PW1 and some other person. However, counsel for the defense objected to the admissibility of the document. The Defence Counsel argued that there was a discrepancy between PW1's viva voce and the certificate sought to be tendered. The discrepancy was considered foundational and in contravention of Section 84 of the Evidence Act, 2011. The discrepancy was related to the model of the device said to have produced the electronic document. The learned Defense Counsel submitted that after comparing the certificate of authentication attached to the printout of the computer-generated evidence (purported conversation between PW1 and some other person via WhatsApp) and parole evidence given by PW1, there was a substantial difference which could not be overlooked as it stood in violation of Section 84 of the Evidence Act. PW1, in his parole evidence, attested that the phone model in which the conversation ensued was a Samsung A5. However, on the certificate of authentication tendered, the device model, as was written and signed by PW1, was a Samsung A7. Counsel for the defence contended that the provisions and conditions stipulated under Section 84 of the Evidence Act must be strictly complied with conjunctively. Failure to comply with any of the requisites results in the inadmissibility of such electronic evidence.[1]

2. Held

The Presiding Judge of the Federal High Court, Yenagoa, Hon. Justice Isa H. Dashen (Judge), on 9 November 2021, delivered a ruling on the admissibility or otherwise of the printout of the WhatsApp conversation. In finding for the defendant, the learned Justice pointed out that the provision of the law that deals with the admission and relevancy or otherwise of computer-generated/electronic evidence is Section 84 of the Nigerian Evidence Act, 2011, as was rightly argued by the Defense Counsel.[2] His Lordship further stated that Section 84 was put in place to ensure that the computer/devices used in producing the documents are proved to be trustworthy. His decision was backed by the fact that the provisions of the section mentioned above had not been complied with as was required concerning electronic evidence. On that ground, His Lordship marked the evidence as tendered but rejected.[3] His Lordship concluded that 'the proponent of electronic evidence must

*By Felix E. EBOIBI, Associate Professor of Cybercrime Law, Faculty of Law, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria. Tel: +2348033175431. Email: felixeboibi@ndu.edu.ng, lixboibi@yahoo.com, felixeboibi@gmail.com

[1] *Federal Republic of Nigeria v. Charlotte Dehli* - Suit No. FHC/YNG/33C/2021 - Before His Lordship Hon. Justice Isa H. Dashen(Presiding Judge), Federal High Court, Yenagoa, Judgment delivered on 9 November 2021(Unreported), 1-12.
[2] Ibid., at 5
[3] Ibid., 9-11

tender a certificate of authentication as well as oral evidence to corroborate the certificate.'[4] The decision of His Lordship in finding for the defense counsel is anchored on the prosecution's non-compliance with the specifications of Section 84(2) of the Evidence Act. The provision provides that oral evidence is required to provide a foundation for computer-generated evidence sought to be tendered before the court, and Section 84(4) of the Evidence Act, creates a requirement of tendering a certificate to authenticate an electronic document further. The certificate must fulfil the following requirements:

i. The witness must identify the document containing the statement.
ii. Describe the manner in which the document was produced.
iii. Furnish the particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer.
iv. Treat or deal with any matter under section 84(2)
v. The certificate must be signed by a person occupying a responsible position in relation to the operation of the relevant device used or the management of the relevant activities.[5]

The reason placed on the issuance of the certificate is to give backing to the foundational evidence already provided in the *viva voce* (required by section 84(2)). Also, it is to ensure and verify the integrity and authenticity of the document's source before the court so the court can rely on it.[6]

3. Comments

It is a well-known fact that computer-generated evidence can easily be tampered with as they are generally prone to manipulations, as was alluded to by Tobi, JSC in the case of *Araka v Egbue.*[7] This has also been identified by courts of other jurisdictions when dealing with electronic evidence. For instance, the Kenyan High Court, in the case of *Williams Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 Others*[8] identifies that the uniqueness of e-evidence renders it particularly prone, by its very nature, to be easily manipulated in an undetectable manner. Thus, both jurisdictions and several others require the production of a certificate of trustworthiness as an essential element of the authentication process before electronic evidence can be admissible in a court of law. The primary issue leading to the decision of the case under review borders on the discrepancy caught by the defense counsel concerning the testimony and the certificate tendered by the prosecution witness, Mr. Liverpool. The details contained in his viva voce and the certificate as to the device from which electronic evidence emanated were at war, as the specific device was not properly identified. PW1 asserted that the device in use was a Samsung A5 in his viva voce, while the certificate tendered, sought to authenticate a Samsung A7, a different model from that attested to in the viva voce of the same witness. The implication of the preceding is simply that the requirements of section 84(2) and (4) had not been adhered to. Seeing that it is expressly stated in Section 84(4)(b) thus: '… such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer'. The implication of non-compliance with the preceding provisions' specifications directly results in the inadmissibility of the electronic evidence sought to be tendered, as compliance with the provision is arguably mandatory. In the case of *Impact Solutions Ltd v. International Breweries Plc*[9] the court expunged computerized documents due to the failure of the party to authenticate and adhere to the provisions of section 84(2) of the Evidence Act. One of the issues raised for determination by the appellants, in this case, was whether the trial court was right to have overruled the objection raised as to the admissibility of Exhibits A, B, C, D, E, E1 and E2 in the appellant's final written address in view of the provision of section 84(1)(2) and (4) of the Evidence Act, 2011. The appellant's counsel argued that the exhibits tendered by the opposing counsel had not met the requirements enshrined under the Act and that the court had the duty to expunge inadmissible evidence and act on legal evidence alone. His Lordship expressed that the exhibits – e-mail correspondence between the parties – fall squarely within the provisions of Section 268 and 84 of the Evidence Act, 2011 as computer-generated documents. He further pointed out that '…the feuding parties starved the lower court of the certificate of authentication of these documents, or the device whence they germinated from, as decreed by the sacrosanct provision of section 84(2) and (4) of the Evidence Act, 2011.' In dismissing the evidence, the court also referenced the gross failure of the parties' witnesses in their viva voce evidence/testimonies, wrapped in their statement on oath, to comply with the mandatory sections 84(2) and (4) of the Evidence Act. His Lordship, Ogbuniya JCA, held: 'In the instant case, the witnesses of the parties, in their statements on oath failed to

[4] Ibid., at 6.
[5] Ibid., at 9-10, Nigerian Evidence Act, s.84(4)
[6] Ibid.
[7] (2003) 17 NWLR (Pt 848) 1
[8] *William Okungu Kitinya v Republic* [2013] eKLR (Miscelleneous Application No. 58 of 2013)
[9] (2018) LPELR-45441 (CA)

comply with the mandatory requirements of section 84 of the Evidence Act, 2011. Therefore, it renders the documents tendered inadmissible.'

Additionally, in the case of *Omokie Emmanuel v FRN*[10] where e-documents marked as Exhibits C1 – C50 were in question, the court held that, in line with section 84(2) and (4) of the Evidence Act, there are necessary foundations or requirements to be laid for admissibility of a computer-generated document. Very similar to the decision in *MD Zahirul Islam v FRN*,[11] the learned Justice said, 'The supporting certification required under section 84(4)(a) and (b) of the Evidence Act are glaringly absent in exhibit A. Similarly, there are no particulars of any device used in the production of exhibits C1 – C50… I therefore have no hesitation in expunging exhibits C1 to C50'. Also expunged by the court for non-compliance specifically with Section 84(2) and (4) of the Evidence Act. Justice Abimbola Osarugue Obaseki-Adejumo, JCA in *Collins Commemex Nigeria Limited & Anor v Skye Bank Plc*,[12] observed that where electronic evidence is sought to be demonstrated, such electronic document must be certified and comply with the preconditions in section 84(2) and (4) of the Evidence Act, 2011. Inclusively, the implication of contradictions in material facts in the issue of electronic evidence has been addressed in the American case of *Clark v Cantrell.*[13] In this case, Cantrell wanted to introduce a computer-generated animation through her expert witness, and an objection was raised, asserting that the video did not accurately reflect the witness's testimony. The trial judge refused to admit the evidence on the ground that it was inconsistent with prior testimony and inaccurately reflected the evidence.

The cases mentioned above have been particular concerning the authentication and identification of the device from which the evidence is obtained, as well as the device's condition. Following suit, it is not unusual that His Lordship's rejection of the evidence sought to be tendered by the prosecution counsel in the case under review. In the circumstances, it is arguably safe to say that since the device the witness testified over stands in solid contradiction from the one appearing on the face of the certificate, the device used in the production of the exhibits had not been properly authenticated. It will not be out of place to consider that the very discrepancy equals a lack of authentication and identification of the electronic device from which the e-evidence emanated, contravening Section 84(2) and (4) of the Evidence Act, which is arguably a mandatory provision as regards computer-generated evidence. If the foundational evidence (viva voce) does not tally with the certificate, there is a smudge on the integrity of the electronic evidence. This provision of the law is arguably mandatory, and the disunity in such a material fact as to the device may be enough reason to expunge the purported produce.

However, it must be stated that His Lordship arguably based his decision on the strict and old position of the law concerning the mandatory requirement of a certificate of authentication under the Nigerian Evidence Act 2011, which works against the interest of justice, as also espoused in the preceding decisions of courts. Contrary to the decision of His Lordship that 'the proponent of electronic evidence must tender a certificate of authentication as well as oral evidence to corroborate the certificate'[14] the recent Court of Appeal judgment in *Okpu v. Trust Bond Mortgage Bank Plc*[15] and Supreme Court judgment of *Daudu v. FRN*[16] shows otherwise. The mandatory nature of a certificate has been relaxed. A party can either produce a certificate of authentication or give oral evidence to authenticate electronic evidence. Moreover, parties can even decide to waive or consent to the non-production of a certificate of authentication. No method of authentication is superior to the other.[17] This position suits the interest of justice compared to the position taken by His Lordship.

Moreover, in light of recent occurrences and the progressive nature of computers and computer-generated evidence, certain jurisdictions have found alternatives and exceptions to the stringent applications of their admissibility rule regarding electronic evidence, which His Lordship should have taken into account when delivering his ruling. In the Indian jurisdiction, for instance, in the case of *Shafi Mohammad v State of Himachal Pradesh,*[18] the certificate requirement under section 64B(4) of the Evidence Act, was held to be procedural and not mandatory and can be relaxed in the interest of justice. It also resounded that 'threshold admissibility of an electronic evidence cannot be ruled out on any technicality if the same was relevant.'[19] Although His Lordship,

[10] (2018) LCN/12459(CA)
[11] (2018) LCN/11085(CA)
[12] (2019) LCN/12750(CA)
[13] *Clark v. Cantrell*, 339 S.C. 369, 520 S.E.2d 528 (2000).
[14] Ibid., at 6.
[15] (2021) LPELR-54554(CA), 74 -77.
[16] (2018) 10 NWLR (Pt. 1626) 169
[17] *Okpu v. Trust Bond Mortgage Bank Plc* (2021) LPELR-54554(CA), 70 -79; *Daudu v. FRN* (2018) 10 NWLR (Pt. 1626) 169
[18] (2018) 2 SCC 801
[19] Ibid.

in the case under review, reasoned that the printout of the electronic evidence is relevant, it rejected its admissibility on technical grounds.

The Kenyan jurisdiction also adopted a new approach wherein electronic evidence does not affect admissibility but weight. The previous position under Section 106B of the Kenyan Evidence Act prescribed the first notable and substantive requirement for the admissibility of e-evidence as the production of a certificate of authentication accompanying any submission of e-evidence. However, Section 78A, a new amendment to the Act, generally provides that e-evidence is admissible without meeting the certificate requirement. It takes on a presumption of admissibility, which allows for the disparate nature of the varying types of electronic evidence. Here, the legislation shifts the focus of authenticity from the issue of admissibility. It suggests that it ought to be considered when determining the weight to be assigned to the e-evidence so tendered and admitted. In the case of *Muruli v Wycliffe Oparanya & 3 ors*[20] the High Court admitted evidence contained in CDs without a certificate of authentication, citing that the absence of the certificate was a mere technicality that ought not to get in the way of justice. In addition, Article 159 of the Kenyan Constitution, 2010, urges the courts to expunge undue technicalities. Similarly, in the United Kingdom, where the real issue as regards electronic evidence was authenticity, in concluding the matter, it was opined that 'this was a matter which was best dealt with by a vigilant attitude that concentrated upon the weight to be attached to the evidence, in the circumstances of the individual case, rather than by reformulating complex and inflexible conditions as to admissibility.'[21] In furtherance of this, the Law Commission's recommendations, the Justice and Criminal Evidence Act, 1999, specifically barred the application of any technology-specific conditions for the admissibility of electronic records.[22] In Tanzania, where there is no provision under their law requiring a certificate or affidavit to prove the reliability of data or the authenticity of electronic record systems used in the creation of the electronic evidence, the authenticity of electronic evidence before its court is not considered as a matter touching directly on admissibility, but on the weight to be attached to the document. In the case of *Mungai*[23] the authenticity of the electronic evidence tendered before the court was considered after it had already been admitted. Here, the veracity of the e-evidence was tested during the evaluation of evidence.

In criticism of the provisions of the Nigerian Evidence Act and in agreement with the practice of the preceding practices, Amuda-Kannike[24] observed that the provisions of Section 84 of the Evidence Act are unnecessarily cumbersome, opining that Section 34 of the Evidence Act, which touches on the subject of evidential weight, is sufficient to address the issue of electronic evidence before the court. Resounding a similar point is the recent case of *Stanbic IBTC Bank Plc v Longterm Capital Ltd & 2 Ors*[25] which expanded the scope of judicial inquiries into section 84 of the Evidence Act, 2011. It is considered a landmark decision touching on the mandatory nature of producing a certificate of authentication as it concerns electronic evidence. It provides an exception to the compulsory requirement of a certificate, which includes when it becomes practicably impossible to produce a certificate of authentication to back up the production of said certificate. In holding the exhibit under question as admissible, the court opined that the law should not become too strict and should make a compromise in the interest and furtherance of justice. Since the certificate ought to be issued based on the belief and best knowledge of the upholder, he or she must be familiar with the workings of a device to make an assertion that authenticates it. In that case, it was considered that when a certificate itself is impossible to get, the absence of such evidence should not equal a denial of other such critical evidence which may be touching on the conclusion of the case.

Drawing from the decisions of the courts in creating exceptions as regards the issuance of a certificate for authentication, it is not farfetched to assume that a prerogative of a similar manner can be applied to the case under review, wherein in the face of a technical error, crucial evidence not be dispensed with on the grounds of inadmissibility, but the error be addressed in relation to the weight to be assigned to the evidence in light of the error. The court's decision in this case invariably works against the interest of justice manifestly. Conclusively, based on the preceding and in line with the position held by several other jurisdictions as discussed, rather than upset the interest of justice by declaring outright inadmissibility of the e-evidence in question, the rejection of

[20] *Muruli v Wycliffe Oparanya & 3 others* (2013) eKLR
[21] Law Commission, The Hearsay Rule in Civil Proceedings (Law Com No 216, Cm 2321, 1993) [3,2,1]
[22] Section 60 of the Justice and Criminal Evidence Act, 1999; Section 69 of the Police and Criminal Evidence Act, 1984
[23] (Unreported) *William Mungai v Cosatu Chumi and Others*, Election Petition No.8 of the 2015 (High Court of Tanzania, Iringa Registry at Iringa)
[24] Prof. Amuda-Kannike 'Admissibility of Evidence as it Relates to Electronic Devises, Social Media and Forensic Science' (2018), *Business Regulations, Law & Practice* Available at https://www.proshare.ng.com/news/Business%Regulations,%20Law%20&%20Practice/Admissibility-Of-Evidence-As-It-Relates-To-Electronic-Devises-Social-Media-And-Forensic-Science-/39484
[25] (2021) LPELR-55610(CA)

which would make or mar a case, should go to the evidentiary weight assigned to the document instead. All other grounds had been laid and appropriately established as to the reliability of the e-evidence. A dismissal based on a procedural technicality and a minor discrepancy should not have been allowed to determine the ruling of His Lordship.