ARTICLE:

Legal issues surrounding the admissibility of electronic evidence in Tanzania

By **Ubena John**

Introduction

This article examines legal issues surrounding the admissibility of electronic evidence in Tanzania. The central thesis is that despite enactment of the laws (Written Laws Miscellaneous Amendment Act, No. 15 of 2007 hereinafter referred to as WLMAA and the Electronic Transactions Act of 2015, herein referred to as ETA) to cater for the admissibility of electronic evidence, there is still a risk of unreliable evidence being admitted. The courts also seem to have applied the laws inconsistently. After presenting the challenges, this article then proceeds to provide some suggestions for improvement.

The law relating to admissibility of electronic evidence: case law and legislation

This section provides an overview of the development of electronic evidence in Tanzania through examining judicial and legislative changes in the area. Before the year 2000, there was neither legislation nor case law dealing with electronic evidence in Tanzania. The admissibility of electronic evidence in Tanzania, was first discussed in 2000 in the case of Trust Bank Ltd.[1]

The judicial gap-filling role

In *Lazarus Mirisho Mafie and M/S Shidolya Tours and Safaris v Odilo Gasper Kilenga alias Moiso Gasper*[2] the judge rightly pointed out that until the year 2000, Tanzania had no law providing for the admissibility of electronic evidence. The gap left by the legislature was filled by judicial law making. In *Trust Bank Ltd v Le Marsh Enterprises Ltd, Joseph Mbui Magari, Lawrence Macharia*[3] (Trust Bank case) the High Court of Tanzania (Commercial Division) was called upon to rule on whether electronic evidence is admissible in the courts of law in Tanzania. In that case, a preliminary objection was raised against the tendering of a computer printout of banker's books. The court had to rule whether the computer printout of a banker's books was admissible. The court observed that Tanzania did not have a law on admissibility of electronic evidence. Admittedly, the court went on to rule that a computer printout of a banker's books was admissible. In a passing comment, the court urged the legislature to enact a law to provide for admissibility of electronic evidence.

It is worth noting that the *Trust Bank* case dealt with admissibility of a computer printout of bankers' books in civil proceedings. It did not address the general admissibility of electronic evidence in both criminal and civil proceedings in Tanzania.

The legislative response

The judicial response to the admissibility of electronic copies of bankers' books in the *Trust Bank* case did not consider the general admissibility of electronic evidence. Thus, the legislature intervened through the enactment of Written Laws Miscellaneous Amendment Act, Act No 15 of 2007 (WLMAA). The WLMAA provided for the admissibility of electronic banker's books or their computer printout in civil proceedings, and general admissibility of electronic evidence in criminal proceedings. Section 35 of WLMAA amended section 76 of the Tanzania Evidence Act (TEA) that defined the term 'banker's books'. The amendment is to the effect that banker's books include those in the form of a data message generated or stored in the computer system or

[1] *Trust Bank Ltd v Le Marsh Enterprises Ltd, Joseph Mbui Magari, Lawrence Macharia* [2002] TLR 44.

[2] *Lazarus Mirisho Mafie and M/S Shidolya Tours and Safaris v Odilo Gasper Kilenga alias Moiso Gasper* Commercial Case No. 10 of 2008, HC Commercial Division at Arusha (Unreported).

[3] *Trust Bank Ltd v Le Marsh Enterprises Ltd, Joseph Mbui Magari, Lawrence Macharia* [2002] TLR 44.

electronic devices. The WLMAA provides for the admissibility of banker's books generated or stored in computer systems and other such digital devices. In admitting the computer printout of banker's books, the law provides certain requirements, namely: (i) that the system itself assures the accuracy of the printout; (ii) that entry was made in the usual and ordinary course of business; and (iii) that the books are in the custody of the bank.[4]

The judicial rejoinder

The WLMAA did not provide for the general admissibility of electronic evidence in civil proceedings. This was pointed out in *Lazarus Mirisho Mafie and M/S Shidolya Tours and Safaris v Odilo Gasper Kilenga alias Moiso Gasper*.[5] This case dealt with the admissibility of a defamatory e-mail. The High Court observed that there was no law that permitted the admissibility of electronic evidence, such as an e-mail, as evidence in a defamation case. The court examined the definition of the 'document' in the TEA and the Interpretation of Laws Act [Cap. 1 R.E 2002] s4. Section 3 of the TEA defines the term document as 'any writing, handwriting, typewriting, printing, photostat, photograph and every recording upon any tangible thing, any form of communication or representation by letters, figures, marks or symbols or by more than one of these means, which may be used for the purpose of recording any matter provided that such recording is reasonably permanent and readable by sight.' Section 4 of the Interpretation of Laws Act [Cap. 1 R.E 2002] provides that 'document' includes any publication and any matter written, expressed, or described upon any substance by means of letters, figures, or marks, or by more than one of those means, which is intended to be used or may be used for the purpose of recording that matter. The court construed these provisions and the definition of the term 'document' and extended it to include e-mail. Consequently, the objection against the admissibility of the e-mail was overruled. In the process, the court examined how to establish the authenticity of e-mail as evidence.

The development observed in *Lazaro Mirisho's* case was discussed in the case of *Exim Bank (T) Ltd v Kilimanjaro Coffee Company*.[6] In the latter case, the High Court of Tanzania Commercial Division was invited to determine whether the printout of an electronic record of banker's books for an overdraft was admissible in evidence. The issues raised were as follows: (a) whether the printout of statements were made in the usual and ordinary course of business of the bank, (b) whether the bank had custody and control of the statements and (c) whether there was proof that the printouts were examined against the original entries and identified to be correct as required by the law.[7] The court stated that there are two certificates required to establish the reliability and authenticity of electronic records of banker's books:[8]

> (1) A certificate to accompany the printout of bank statements. This certificate should state that it is a true copy of the statement; that the entries were made in the usual and ordinary course of business, and they are in the custody and control of the bank.
>
> (ii) Another certificate should certify that the electronic process through which the statements were generated ensured the accuracy of the printout. The printout should also be signed by the principal accountant or the manager of the bank.

The court further stated that apart from the certificate signed by the principal accountant or the bank manager, there must be a certificate signed by a system administrator (a person in charge of computer system). This certificate should describe the system and explain:[9]

> (i) The safeguards in place to ensure that only authorized persons entered the data or operated the system.
>
> (ii) The measures adopted to ensure data integrity, including preventing and detecting unauthorized data change.
>
> (iii) The mechanisms for data recovery or retrieving lost data due to system malfunctioning.

[4] See TEA s78A (1).
[5] Commercial Case No. 10 of 2008 (HC Commercial Division at Arusha) (Unreported).
[6] Commercial case No 29 of 2011 (HC Commercial Division at Dar es salaam) (Unreported).
[7] TEA s79.
[8] Commercial case No 29 of 2011 (HC Commercial Division at Dar es salaam) (Unreported) at pages 8-11.
[9] Commercial case No 29 of 2011 (HC Commercial Division at Dar es salaam) (Unreported) at pages 10-11.

(iv) The manner of data transfer from the system to removable devices.

(v) The identification mode used to identify the storage devices.

(vi) Any other facts that will help to verify accuracy and integrity of the system and data.

Moreover, the court said the system administrator should certify that to the best of his knowledge, the system operated well at the material time. The court refused to admit the printout statement of the bank account. It held that it is necessary to establish the authenticity of the electronic banker's record before admitting it into evidence. It is worth noting that the *Exim Bank's* case was the first case in Tanzania to lay down a procedure to establish the reliability and authenticity of electronic evidence, particularly banker's books in electronic form.

The enactment of the electronic evidence law

In 2015, the legislature in Tanzania enacted the Electronic Transactions Act (ETA).[10] The ETA was enacted to provide for the admissibility of electronic evidence in any proceedings. Its long title states as follows:

> 'An Act to provide for legal recognition of electronic transactions, e-Government services, the use of Information and Communication Technologies in collecting evidence, admissibility of electronic evidence, to provide for the use of secure electronic signature; and provide for other related matter.'

In dealing with electronic evidence, the ETA defines fundamental terminologies such as data, data message, document, electronic evidence, etc. It further provides for a functional equivalence rule – that is, electronic evidence is like any other documentary evidence, and is admissible. Thus, electronic evidence should not be denied admissibility because it is a data message, as set out in s18(1):

> 18.-(1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility of data message on ground that it is a data message.

Moreover, the ETA provides criteria for determining the reliability, admissibility, authenticity and assessing the weight of a data message, as set out in 18(2). It also provides criteria for admitting electronic records in evidence, as set out in 18(3). After the enactment of the ETA, as discussed below, several cases were filed in which the application of that law was tested.

The judicial application of the electronic evidence law

The first case to put the ETA to test was *William Mungai v Cosatu Chumi and Others*.[11] In this case, a preliminary objection was raised against admission into evidence of an audio CD, which was tendered as evidence with regards to an interview conducted between Ebony radio and the first respondent. The court was of the view that ETA s18(2) provides for determining the weight to be given to electronic evidence, and s18(1) provides for the admissibility of electronic evidence. The court admitted the audio CD in evidence because it was satisfied that the witness who tendered the CD possessed the requisite knowledge that met the requirements set out under the ETA s18(2). However, it may be observed that in this case, the court admitted the audio CD in evidence before testing the veracity or reliability of the evidence.[12]

The second case to interpret the ETA was *Emmanuel Godfrey Masonga v Edward Franz Mwalongo*.[13] This was a case in which a party wished to tender a video CD (VCD) in evidence. The other party raised a preliminary objection that the content of the VCD was inadmissible because it was neither reliable nor authentic. The court upheld the preliminary objection. The VCD sought to be tendered was translated from a video clip which was recorded on a mobile telephone. The original mobile telephone on which the video clip was recorded was lost. Before the mobile telephone

[10] Act No.13 of 2015.

[11] Election Petition No.8 of 2015 (Hight Court of Tanzania, Iringa Registry at Iringa) (Unreported).

[12] Ubena John, 'ICT Law – A discipline without jurisprudence?', Institute of Judicial Administration, Lushoto, Journal 1/1(2017)19; see also Ubena John, 'Legal Issues surrounding tendering of electronic evidence in the courts of law in Tanzania,' Paper presented during TLS Morogoro chapter seminar 28 December 2018, at Cherry Hotel Morogoro, Tanzania.

[13] Miscellaneous Civil Cause No. 6 of 2015 (High Court of Tanzania at Njombe) (Unreported) ruling delivered on 4 April 2016.

was lost, the witness (PW6) sent the video clip to the petitioner. Thereafter, the petitioner sent the video clip to the new mobile telephone of the witness (PW6). The video clip was then translated into the VCD, which was sought to be admitted in evidence. The court was concerned that there was no police loss report. The model of the mobile telephone was never stated. The court consequently refused to admit the video clip into evidence, because its reliability and authenticity were doubtful.[14]

The court's view was that the requirements of ETA s18(2) were not satisfied because there was risk of manipulation of content of the VCD. Moreover, there was no evidence that other persons could not have obtained access to the VCD and subsequently altered its content. The manner of communication from PW6 to the petitioner and from the latter to PW6 did not eliminate the risk of manipulation. This may appear to be a controversial ruling, because there was no evidence to demonstrate that anybody had the motive to alter the evidence, nor was there evidence to suggest the evidence was altered. However, the defendant may simply show doubt in a particular testimony or evidence, and in this case, the judge determined that the proponent had failed to provide sufficient evidence to assuage the doubt.

More importantly was the court's remarks that before admitting electronic evidence, it is necessary to give an account of the reliability and authenticity of the data. It follows that before admitting electronic evidence, an account of its reliability is necessary. This includes displaying reliability before the court and satisfying the court of the reliability of the evidence.[15]

The changes brought by the law

The following discussion highlights some of the changes that the law brought regarding electronic evidence in Tanzania. These changes range from a rule permitting the admission of electronic evidence in the courts of law in Tanzania, to the presumption of the authenticity of an electronic records system.[16]

Admissibility of electronic evidence

Section 64 of the TEA deals with primary documentary evidence (original documents). The primary evidence is the document itself, produced for the inspection of the court.[17] A document in electronic or digital form (text, image, sound, video, or their combination) may be documentary evidence. It is noted above that the *Le Marsh* case admitted computer printouts of banker's book as evidence, and the WLMAA provided for the admissibility of electronic evidence in criminal proceedings. It further allowed admission of banker's books in electronic form or a printout as evidence. The TEA, as amended by ETA, provides for the admissibility of electronic evidence. Section 46 of the ETA adds a new provision in the TEA: s 64A. Section 64A (1) provides that '…In any proceedings electronic evidence shall be admissible.' Moreover, TEA s64A(2) states that '…The admissibility and weight of electronic evidence shall be determined in the manner prescribed under ETA s18...' Providing for the admissibility of electronic evidence was an important step.

The functional equivalence principle

Another vital change the ETA has brought is the introduction of a 'functional equivalence principle.' Under this principle, evidence in electronic form (including computer printouts) can comprise documentary evidence.[18] It means that the evidence cannot be denied admissibility because it is in electronic form. This removes uncertainty and discrimination regarding electronic evidence. It is now settled law that electronic evidence is admissible in any proceedings.[19]

Definition of 'electronic evidence'

The TEA was amended to introduce, among other things, a new term: 'electronic evidence'. Section 64A of the TEA defines 'electronic evidence' as any data or information stored in electronic form or electronic media or retrieved from a computer system which can

[14] See also Ubena John, 'ICT Law – A discipline without jurisprudence?', Institute of Judicial Administration, Lushoto, Journal, 1/1(2017), 19-21.
[15] Miscellaneous Civil Cause No. 6 of 2015 (High Court of Tanzania at Njombe) (unreported); See also Ubena John, 'ICT Law – A discipline without jurisprudence?', Institute of Judicial Administration, Lushoto, Journal 1/1(2017), 19.
[16] See also Alex B. Makulilo, 'Admissibility of computer evidence in Tanzania', *Digital Evidence and Electronic Signature Law Review* 4 (2007), 56-60; Adam J. Mambi, 'Electronic evidence in Tanzania', *Digital Evidence and Electronic Signature Law Review* 10 (2013), 123-127; Zakayo Lukumay, 'Foundation for admissibility of electronic evidence in Tanzania', *Law School of Tanzania Law Review*, 1/1(2016), 148-185.
[17] TEA s64(1).
[18] ETA of 2015 s18(1).
[19] ETA s18(1).

be presented as evidence.[20] It may further be noted that both s40A and s78A of the WLMAA, together with s64A of the TEA recognise the existence of electronic documents or records that may be admitted as evidence.

Broadened definition of a 'document'

The definition of the term 'document' was broadened to include data in electronic form.[21] The legislature also made changes to the definition of the term 'document' under TEA s3 (TEA R.E. 2019) to include data in electronic form. This is a new development in Tanzania. The broadening of the definition of the term 'document' implies that data such as text, SMS, e-mails, sound (voice notes), video (video clips), and a combination of these, may be admitted as documentary evidence.

Criteria for determining admissibility and weight of electronic evidence

To guide litigants, lawyers and the court on the features of electronic evidence to be admitted into legal proceedings, the law set the criteria for determining admissibility and the weight of such evidence (ETA s18(2)). Thus, besides broadening the definition of the term 'document' and considering the nature of electronic evidence – that is, the risk of manipulation, the legislature in Tanzania introduced criteria for determining admissibility and the weight of electronic evidence. These are set out under ETA s18(2). The provision provides that '…In determining admissibility and evidential weight of a data message, the following shall be considered-

> (a) the reliability of the manner in which the data message was generated, stored or communicated.
>
> (b) the reliability of the manner in which the integrity of the data message was maintained.
>
> (c) the manner in which its originator was identified; and
>
> (d) any other factor that may be relevant in assessing the weight of evidence.'

The presumption of authenticity of an electronic record system

Another change included a presumption of authenticity of electronic record system. The ETA s18(3) provides that:

> 'The authenticity of an electronic records system in which an electronic record is recorded or stored shall, in the absence of evidence to the contrary, be presumed where -
>
> (a) there is evidence that supports a finding that at all material times the computer system or other similar device was operating properly[22] or, if it was not, the fact of its not operating properly did not affect the integrity of an electronic record and there are no other reasonable grounds on which to doubt the authenticity of the electronic records system;
>
> (b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

[20] TEA s64A (3).

[21] See *Mirisho's* case: the meaning of a document extends to e-mail; see also ETA s18(1).

[22] The words 'operating properly' have not been defined under the ETA. The term 'operating properly' may be ambiguous, as it does not necessarily mean absence of bugs, for which see Chapter 6 in Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), open source at https://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence; Peter B. Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 1-14; Peter B. Ladkin, 'Robustness of software', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 15-24; Paul Marshall, 'The harm that judges do – misunderstanding computer evidence: Mr Castleton's story – an affront to the public conscience', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 25-48 and James Christie, 'The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 49-70.

(c) it is established that an electronic record was recorded or stored in the usual and ordinary course of business[23] by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.'

The provisions of TEA s18(3) pose a challenge. This is because the judge is the one who decides that the electronic record system was 'operating properly'. There is no statutory guidance regarding the meaning of 'operating properly'. A judge will have to take evidence from witnesses that have the appropriate competence, knowledge and qualifications to explain this in respect of the evidence to be adduced. Fraser J had to consider this matter in *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1*.[24] Anthony de Garr Robinson QC for the Post Office asserted, in his opening speech, that the Horizon system was 'robust'.[25] Fraser J discussed 'robust' at [36]-[56] and concluded at [936]:

'I consider, as explained in the Technical Appendix, that Legacy Horizon was not robust, and that although Horizon Online in its HNG-X form was better than Legacy Horizon (not least, I consider, because Riposte was no longer part of Horizon) its robustness was questionable and did not justify the confidence placed in it by the Post Office in terms of its accuracy.'

Fraser J further concluded, at [977]:

'In summary terms only, Legacy Horizon was not remotely robust. The number, extent and type of impact of the numerous bugs, errors and defects that I have found in Legacy Horizon makes this clear.'

The nature of the evidence that the parties will have to submit to a judge to reach a determination on the meaning of 'operating properly' will depend on the nature of the electronic evidence before them. By way of example, in a banking case in civil proceedings, it will be necessary to ascertain relevant evidence at the disclosure stage.[26] In criminal proceedings, the approach will be slightly different, because consideration will need to be given to the integrity of the first-in-time evidence.[27] In this respect, it will be necessary to consider some or all of the tests set out in paragraph 7.128 of Mason and Seng,[28] as replicated in article 4 of the Draft Convention on Electronic Evidence.[29]

The role of standards

Another important addition to the law in Tanzania is the recognition of the roles of standards (procedures, usage or practice on how electronic records are to be recorded or preserved depending on the nature of business or endeavour) in determining the admissibility of electronic evidence. The ETA s18(4) provides as follows:

'For purposes of determining whether an electronic record is admissible under this section, an evidence may be presented in respect of any set standard, procedure, usage or practice on how electronic records are to be recorded or stored, with regard to the type of business or endeavours that used, recorded or stored the electronic record and the nature and purpose of the electronic record.'[30]

[23] The phrase 'in the usual and ordinary course of business' has not been defined under the ETA s18(3)(c).
[24] [2019] EWHC 3408 (QB), available at http://www.bailii.org/ew/cases/EWHC/QB/2019/3408.html
[25] Note: the word 'reliability' was also used in this case and discussed by the judge – both words were used almost interchangeably. However, consider the technical criticism levelled against the comments made by Anthony de Garr Robinson QC in his opening speech, set out in a review of Charles Morgan, *Responsible AI: A Global Policy Framework* (2019, United States of America, International Technology Law Association) in Book Reports, *Digital Evidence and Electronic Signature Law Review* 16 (2019), 107-113.
[26] As set out in Paul Marshall, James Christie, Peter B. Ladkin, Bev Littlewood, Stephen Mason, Martin Newby, Jonathan Rogers, Harold Thimbleby and Martyn Thomas CBE, 'Recommendations for the probity of computer evidence', *Digital Evidence and Electronic Signature Law Review* 18 (2021), 18-26, at 24-25.
[27] Referred to in Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017) at 7.92 and 9.33.
[28] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017).
[29] *Digital Evidence and Electronic Signature Law Review* 13 (2016), S1-S11.
[30] In comparison to the Tanzania ETA s18(4), the Malaysia Evidence Act 1950 s90A(1) requires evidence of a certificate

Even though the ETA s18(4) has not been tested in judicial proceedings yet, the inclusion of a similar provision in the Commonwealth Model Law on Electronic Evidence (s8) underlines its usefulness.

Evidence to support the authenticity of electronic records system

In appreciating that the electronic records system may have inherent bugs or may lead to errors in the electronic record, the law in Tanzania requires, for the presumption to be exercised under ETA s18(3), that a party wishing to rely on it should provide evidence to show that the system was operating properly. The need for evidence to prove that the computer system was operating properly and if it was not operating properly it did not affect the integrity of the electronic records (ETA s18(3)(a)) has, it is suggested, solved the problems that England & Wales is facing due to a blunt presumption that the computer system operates properly in absence of evidence to the contrary,[31] and the repeal of the requirement for evidence to support the integrity of a computer system.

Incomplete law?

There are areas where the law on electronic evidence in Tanzania is incomplete. The following discussion proceeds to provide a rationale and justification to support this observation. There are several scholarly works on the incompleteness of the law,[32] but the law generally ought to be complete for legal certainty and legitimacy purposes.

A witness need not be a digital evidence professional

From a review of the law and scholarly works, the law in Tanzania seems to be incomplete and inconsistent with the view held by legal scholars in the area. The Tanzania law provides for the admissibility or the handling of electronic evidence without involving digital evidence professionals. The absence of such necessary evidence means there is a risk that Tanzania will be affected by similar scandals as in the English Post Office Horizon scandal.[33]

While it is not necessary to have legislation for the involvement of a digital evidence professional in admitting electronic evidence, it may be vital to bring them as witnesses in the trial involving electronic evidence. It is important to appreciate that adducing electronic evidence requires expertise. The trained operator of the machine (computer driven device) should be preferred to the untrained operator. Some things will not be known by the computer system user. It means that not just any operator of an electronic device will be able to detect if the device was malfunctioning in any way.[34] Similarly, in the

('shall' be proof of the authenticity and reliability of its contents) produced under s90A(1) of the Act, or by calling the maker of the document, electronic record or sender of e-mail to testify; see Gits Radhakrishna, 'E-mail, and the hearsay rule – commentary on Malaysian case', *Digital Evidence and Electronic Signature Law Review*, 10 (2013), 109.

[31] *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB); Peter B. Ladkin, 'Robustness of software' *Digital Evidence and Electronic Signature Law Review* 17 (2020), 15-24 . See also Paul Marshall, 'The harm that judges do – misunderstanding computer evidence: Mr Castleton's story – an affront to the public conscience', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 25-48. See also Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), Chapter 6.

[32] Pistor and Xu, 'Incomplete law', 35 N.Y.U.J. INT'L L. & POL. 931 (2003).

[33] See *William Mungai v Cosatu Chumi and Others*, Election Petition No.8 of 2015 (Hight Court of Tanzania, Iringa Registry at Iringa) (Unreported).

[34] Stephen Mason and Daniel Seng, editors, Electronic Evidence (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 118; see, in particular, Chapter 10 'Competence of witnesses. See also Eric Van Buskirk and Vincent T Liu, 'Digital evidence: challenging the presumption of reliability' (2006) 1 *Journal of Digital Forensic Practice,* 19; Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 1-14; Peter B. Ladkin, 'Robustness of software' *Digital Evidence and Electronic Signature Law Review* 17 (2020), 15-24; James Christie, 'The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 49-70; Paul Marshall, James Christie, Peter B. Ladkin, Bev Littlewood, Stephen Mason, Martin Newby, Jonathan Rogers, Harold Thimbleby and Martyn Thomas CBE, 'Recommendations for

Australian case of *Bevan v The State of Western Australia*[35] the majority decision was that the work of the programmer is immaterial. Nevertheless, Buss J (in the minority) rightly took a different view. He rejected the evidence given by the constable (the operator of the machine) partly because he was not qualified to comment on the software as he was not its developer.[36] This helps to avoid a naïve assumption that computer systems are reliable. After all, the errors in the computer system may be caused by poor software installation, software code errors due to programming or operational errors. Thus, there may be human errors, inherent software bugs, etc. These may consequently lead to system failure, inaccessibility of the system-controlled services or an error in the electronic records.[37]

While digital evidence professionals fall under the provision of expert testimony,[38] the court in Tanzania has held that in tendering electronic evidence, the witness tendering electronic evidence need not be an expert.[39] It means that the digital evidence professional may be excluded in the process of determining the admissibility of electronic evidence. But as already explained, the failure to admit evidence from a suitably qualified digital evidence professional poses a risk that evidence tendered and admitted to the court may not be authentic because generally such evidence is malleable, mutable, and ephemeral in nature.[40]

Admitting electronic evidence without laying the foundation

Challenges on the interpretation and application of ETA s18(2) and (3) has manifested itself in the case law. This led to two schools of thought. The first one takes a stand that electronic evidence should not be admitted unless the foundation of the evidence (proven reliability and authenticity of the evidence) has been successful. There are two cases supporting this school, the *Exim Bank's* case and *Mwalongo's* case. The second school requires no foundational evidence before determining admissibility of evidence. In other words, the authenticity of evidence should be determined after evidence has been admitted. This is the view taken in *Mungai's* case. That is, admit the data message then test its veracity during evaluation of evidence (*Mungai's* case). Moreover, reading the precedents (*Mungai's* case*; Mwalongo's* case and *Exim Bank's* case) it is clear that there is an inconsistency in the way judges treat the laying of the foundation in terms of electronic evidence. In some cases they require such foundation to be laid before admitting the electronic evidence, and in other instances they admit electronic evidence without demanding a foundation to be laid (*Mungai's* case). Had the statutory law(s) been complete, such inconsistency could have been avoided.

Shortcomings in the law

Some provisions of the law seem to be wrong. Firstly, consider the practice that whenever electronic evidence is tendered, the party tendering it must prove the reliability and authenticity of the evidence; and the party raising a preliminary objection has no obligation to prove unreliability or non-authenticity of the evidence.[41] The burden of proof rests, as is normal, on the party tendering the evidence. Arguably, because there is so much ignorance of evidence in electronic form, it is easy for the objecting party to simply point to areas where doubt could arise without providing evidence of unreliability of the evidence. Truly, the general rule of evidence is that the party who alleges must prove, as set out in s110 of the TEA:

> **Burden of proof**
>
> 110.-(1) Whoever desires any court to give judgement as to any legal right or liability

the probity of computer evidence', *Digital Evidence and Electronic Signature Law Review* 18 (2021), 18-26.

[35] [2012] WASCA 153.

[36] See also Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 119 see Chapter 6 in particular for examples.

[37] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 123-124.

[38] TEA s47.

[39] See *William Joseph Mungai v Cosato David Chumi and Others*, Misc. Civil Cause (Election Petition) No 8 of 2015, High Court of Tanzania, at Iringa (Unreported).

[40] For characteristics and challenges of digital evidence, see Stephen Mason and Allison Stanfield, 'Authenticating electronic evidence', in Mason and Seng (eds), *Electronic Evidence*, 193-258 at 194-200.

[41] See ETA s18(2); *Emmanuel Godfrey Masonga v Edward Franz Mwalongo* Miscellaneous Civil Cause No. 6 of 2015 (High Court of Tanzania at Njombe) (Unreported) ruling delivered on 4 April 2016.

> dependent on the existence of facts which he asserts must prove that those facts exist.
>
> (2) When a person is bound to prove the existence of any fact, it is said that the burden of proof lies on that person.
>
> **On whom burden of proof lies**
>
> 111. The burden of proof in a suit proceeding lies on that person who would fail if no evidence at all were given on either side.
>
> **Burden of proof of particular fact**
>
> 112. The burden of proof as to any particular fact lies on that person who wishes the court to believe in its existence, unless it is provided by law that the proof of that fact shall lie on any other person.

The other party may raise doubts to discredit the reliability and authenticity of the evidence tendered.

Secondly, there is discrepancy in the laws, especially on the need to provide evidence to prove that at the material time the electronic record system was operating properly. While ETA s18(3) requires such evidence, the TEA s40A and WLMAA s33 seem to provide a different position on electronic evidence obtained in under a cover operation (such as surveillance systems). The latter arguably means that the system used to generate electronic evidence in undercover operations are more authentic or should be trusted, which may not always be the case.[42] There are several cases and scholarly works that confirm that generally computer system is unreliable.[43] For that reason, we appreciate that ETA requires that when data (electronic records) generated from computer system is tendered as evidence, a proof that the computer system was operating properly or the fact of it not operating properly did not affect the reliability and authenticity of records must be given.[44]

As above noted, in Tanzania, a need for the intrinsic evidence to prove the reliability of computer systems is not emphasized in the WLMAA (this law has neither been amended nor repealed, indeed, its provisions have been included in the TEA Revised Edition of 2019), which poses a danger for admitting evidence generated from a dysfunctional computer system or a system that is prone to errors. Ladkin has discussed this in detail.[45] From his work, it is clear that computer systems are prone to errors. Furthermore, several authors have made a detailed discussion on the presumption that a computer system was operating properly.[46] However, in Tanzania although there is a qualified presumption of authenticity of an electronic record system,[47] the law – controversially – regards the electronic record of banker's books as primary documentary evidence (the best evidence),[48] provided it was made in the usual and ordinary course of business, and the book is in the custody of the bank.[49]

On the authenticity of an electronic records system, section 18(3) of the ETA, which is similar to the Model

[42] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 6.150 where this specific problem is illustrated in relation to interception of communications and problems with software and hence the reliability of the electronic evidence.

[43] See *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB); Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), Chapter 6. See also James Christie, 'The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence', *Digital Evidence and Electronic Law Signature Review* 17 (2020), 49-70; Paul Marshall, 'The harm that judges do – misunderstanding computer evidence: Mr Castleton's story – an affront to the public conscience', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 25-48; Peter B. Ladkin, 'Robustness of software', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 15-24; Peter B. Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 1-14.

[44] See ETA s18(3).

[45] Peter B. Ladkin, 'Robustness of software', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 15-24.

[46] See Paul Marshall, 'The harm that judges do – misunderstanding computer evidence: Mr Castleton's story – an affront to the public conscience', 17 (2020), 25-48; Peter B. Ladkin, 'Robustness of software', *Digital Evidence and Electronic Signature Digital Evidence and Electronic Signature Law Review Review* 17 (2020), 15-24; the Commonwealth Model Law on Electronic Evidence s7 deals with the presumption of integrity.

[47] ETA s18(3).

[48] TEA s78A(2).

[49] TEA s78(2).

Law on Electronic evidence,[50] provides that the authenticity of electronic record shall be presumed[51] where:

> (a) there is evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of an electronic record and there are no other reasonable grounds on which to doubt the authenticity of the electronic records system;
>
> (b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or
>
> (c) it is established that an electronic record was recorded or stored in the usual and ordinary course of business[52] by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.'

If the party wishes to rely on the presumption under s18(3), it is necessary for them to bring the evidence to show that the system that generated the data/electronic record was operating properly. If they are successful, the presumption will stand unless the objecting party provides the evidence to rebut it. However, the party challenging the presumption faces the same hurdle as in England & Wales, as pointed out by Mason: 'The problem for the lawyer making the challenge is that only the party in possession of the electronic evidence has the ability to understand fully whether the computer or computers from which the evidence was extracted can be trusted.'[53] In addition, the English presumption asserts something positive, but so does the Tanzanian legislation, also pointed out by Mason: 'The third problem is that the presumption asserts something positive. The opposing party is required to prove a negative in the absence of relevant evidence from the program or programs that are relied upon. In criminal proceedings, this has the unfair effect of undermining the presumption of innocence, and in civil proceedings the party challenging the presumption must convince a judge to order up the delivery of the relevant evidence, including software code, if the evidence is to be tested properly.'[54]

Besides the controversies noted above, it is important to note the terminological variation between what is stated in ETA s18(3) on 'presumption of authenticity of electronic records system', and the Commonwealth Model Law on Electronic Evidence s7 on 'presumption of integrity of electronic records system'. The former used the word 'authenticity' and the latter has the word 'integrity.' These words have different meanings. Integrity presupposes that the data or system is unchanged or has not been altered.[55] According to Mason and Seng, integrity refers to wholeness and soundness of a document. It means a document is complete and uncorrupted in its lifecycle. It thus relates to organization's control over the preservation of a document.[56] In the context of the presumption cited, the focus is on the integrity of the

[50] The Commonwealth Model Law on Electronic Evidence is available at https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_7_ROL_Model_Bill_Electronic_Evidence_0.pdf

[51] For the position in England & Wales, see Paul Marshall, 'The harm that judges do – misunderstanding computer evidence: Mr Castleton's story – an affront to the public conscience', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 25-48; Peter B. Ladkin, 'Robustness of software', *Digital Evidence and Electronic Signature Law Review* 17 (2020), 15-24. See also Stephen Mason and Daniel Seng, editors, Electronic Evidence (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), Chapter 6.

[52] The phrase in the usual and ordinary course of business has not been defined under the ETA s18(3)(c).

[53] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 6.194.

[54] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 6.202; see also 6.222-6.224.

[55] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 7.15.

[56] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 7.92.

electronic records system. Thus, the 'integrity' of the electronic records system seems to be the appropriate phrase because 'authenticity' relates to the electronic records/data themselves and not the electronic records system.[57] Thus the integrity of electronic records depends on the integrity of the electronic records systems.

Authenticity, on the other hand, means something genuine or authentic. Mason and Seng dealt with authenticity of electronic records as evidence.[58] To prove authenticity of an electronic document the creator or the keeper of the document should be called upon to testify.[59] To complicate the situation further there is a term 'reliability'. This is often used in the context of systems that contain digital data that may be produced as evidence.[60] The presumption of reliability or integrity of an electronic records system may aid authentication of electronic records it carries or stores.[61]

Proof by affidavit/certificate of authenticity

Yet another gap in the law in Tanzania is the lack of provision requiring a certificate or affidavit in establishing the reliability of data and authenticity of electronic records systems. A good thing about the certificate or affidavit is that it will be submitted by a digital evidence professional. In other instances, it may be a person in charge of a computer system in a particular organisation. Understandably, where large and complex systems are involved it may be problematic, as illustrated in the *Bates case*.[62] Although the general rule of evidence provides that evidence may be adduced orally or by way of an affidavit, for the sake of clarity the same could have been included in the ETA to save people from cross referencing to other pieces of legislation. For instance, the Civil Procedure Code Act [Cap.33 R.E 2002] provides a general rule that the court may order any point to be proven by affidavit.

In the absence of a provision requiring an affidavit in the ETA, it appears that an affidavit or certificate produced under sections 18(2) and 18(3) of ETA to prove authenticity of electronic evidence is done by way of cross referencing to the Civil Procedure Code Act [Cap.33 R.E 2002].[63]

There is also lack of proper or precise format for presenting a document or the evidence for laying down the foundation of electronic evidence. However, the judges have attempted to provide the format of the certificate that may be used for presenting electronic evidence.[64] But these efforts have neither been sanctioned by the Court of Appeal of Tanzania nor prescribed by the legislature. Unlike the laws of Tanzania, s9 of the Commonwealth Model Law on Electronic Evidence clearly mentions proof by affidavit, and s10 provides for the possibility of the deponent being cross examined.[65]

Compounded by the absence of proof of matters in ETA s18(2) and s18(3) by affidavit, the dilemma centres around the format of such a certificate or affidavit. Two cases reveal the problem, *the Exim Bank*

[57] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 7.84.
[58] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), (6.159, 7.15.and 7.16).
[59] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), (6.159, 7.15.and 7.43)
[60] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), Chapter 6.
[61] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), 6.192.

[62] *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1*[2019] EWHC 3408 (QB).
[63] Order XIX Rule 1 of the Civil Procedure Code Act [Cap.33 R.E 2002].
[64] *Exim Bank (T) Ltd v Kilimanjaro Coffee Company*, Commercial case No 29 of 2011 (HC Commercial Division at Dar es salaam) (Unreported). See also *Emmanuel Godfrey Masonga v Edward Franz Mwalongo* Miscellaneous Civil Cause No. 6 of 2015 (High Court of Tanzania at Njombe) (unreported) ruling delivered on 4 April 2016.
[65] Although the Model Law is helpful, it has not drawn a link between electronic evidence and expert testimony. In many legal systems these have been separated. Also, the conditions given for one to rely on the presumption of integrity under s7 of the Model law dilutes the presumption. One may suggest that, if possible, the presumption be removed as s7 will still be effective without the presumption. The provision could therefore be 'integrity of electronic records system'. The provision on electronic signature (s12) is brief and may be removed as in some jurisdictions electronic signature law exist.

Ltd's case and *Mwalongo's* case.[66] In both cases, two certificates were required (one from the person in charge of the computer system of a particular institution, and another from the head of the institution/unit, e.g. for a bank it might be the branch manager). It is doubtful whether these officers will be digital evidence professionals. But the assumption of the judges is that considering their position in the organisation, they are competent witnesses. Nevertheless, it is debatable whether such people have the requisite qualifications to give evidence on electronic evidence.[67] However, there are instances where in addition to the two certificates, the computer system user may be required to swear an affidavit. This makes a total of three certificates or affidavits. Thus, the case law has confused lawyers in Tanzania, and at the moment they do not know which approach to take. Moreover, the legislation has not prescribed the content of these certificates or affidavits. Consequently, it has created uncertainty in the court procedures.

To sum up, while the changes in the law are appreciated, there remain problems with the admissibility of electronic evidence in Tanzania. To mention but a few, there is no foundational evidence, no, or rare involvement of a digital evidence professional, no provision prescribing an affidavit and its format.

Concluding remarks

To conclude, the law has brought about several good changes, including providing for the admissibility of electronic evidence; defining electronic evidence, and the case law has broadened the definition of the term 'document'. Moreover, the law has provided for a conditioned presumption of the authenticity of electronic records systems.

Despite these changes to the law, a number of crucial matters are missing in the law. Namely, the requirement of foundational evidence in admitting electronic evidence, proof by affidavit with respect to matters stated in ETA s18(2) and (3), and the format of the affidavit. In addition, it is evident that the interpretation of the presumption under ETA s18(3) is inaccurate, because a court presumes evidence is reliable without requiring the party tendering the evidence to prove the reliability of the evidence. This is a highly significant problem, because judges do not appear to understand the need for the disclosure of relevant data. Admitting electronic evidence without involving a digital evidence professional cannot be right. The latter practice poses a risk of admitting evidence that is not authentic.

To address these challenges, it is suggested that, to ensure there is a fair trial, the disclosure of data is mandatory, as set out in Marshall.[68] In addition, the law should prescribe that the matters referred to in ETA s18(2) and s18(3) may be established by an affidavit or certificate, and its content or format be provided. It should be normal for a digital evidence professional to be involved in any dispute where the admissibility of digital evidence is disputed, and finally, the tendering of additional evidence (where necessary) to prove the authenticity of an electronic records system should be ubiquitous.

Ubena John, LL.M, LL.D. (ICT Law) is a Dean, Faculty of Law, Mzumbe University, Tanzania.

E-mail: jubena@mzumbe.ac.tz

[66] *Exim Bank (T) Ltd v Kilimanjaro Coffee Company*, Commercial case No 29 of 2011 (HC Commercial Division at Dar es salaam) (Unreported). See also *Emmanuel Godfrey Masonga v Edward Franz Mwalongo* Miscellaneous Civil Cause No. 6 of 2015 (High Court of Tanzania at Njombe) (unreported) ruling delivered on 4 April 2016.

[67] For qualifications see Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS and Humanities Digital Library, School of Advanced Study, University of London, 2017), Chapter 10. See also 7.59.

[68] Paul Marshall, James Christie, Peter B. Ladkin, Bev Littlewood, Stephen Mason, Martin Newby, Jonathan Rogers, Harold Thimbleby and Martyn Thomas CBE, 'Recommendations for the probity of computer evidence', *Digital Evidence and Electronic Signature Law Review* 18 (2021), 18-26 for the two-stage requirement.