ASSESSMENT OF CHALLENGES OF DIGITAL TECHNOLOGY IN ADMISSIBILITY OF ELECTRONIC EVIDENCE IN TANZANIA

EDWIN MWOMBEKI KAMALEKI

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR DEGREE OF MASTER OF LAWS IN INFORMATION AND COMMUNICATION TECHNOLOGY LAW

(DEPARTMENT OF PRIVATE LAW)

OF THE OPEN UNIVERSITY OF TANZANIA

2024

CERTIFICATION

The undersigned certify that they have read and hereby recommend for acceptance by the Open University of Tanzania a dissertation titled: “Assessment of challenges of digital technology in admissibility of electronic evidence in Tanzania” in partial fulfilment of the requirements for the Degree of Master of Laws (Information Communication Technology (ICT).

..……

Dr. Rindstone Ezekiel

(Supervisor)

……

Date

……..……

Dr. Saphy Bullu

(Supervisor)

……

Date

COPYRIGHT

DECLARATION

I, **Edwin Mwombeki Kamaleki,** declare that, the work presented in this dissertation is original. It has never been presented to any other University or Institution. Where other people's works have been used, references have been provided. It is in this regard that I declare this work as originally mine. It is hereby presented in partial fulfilment of the requirement for the Degree of the Master of Laws in Information Communication Technology (LL.M).

.....

Signature

.....

Date

DEDICATION

This dissertation is dedicated to my parents: My father Mr. Faustine Mwesiga Kamaleki who is sick for the period of good eleven (11) years and is bedridden to date. This dedication carries a prayer to almighty God to reduce his pain and promote his quick recovery. Again, my dedications extend to my Mother Winfred Kokutangilila Kamaleki who without her loves and courage this work would have become futile. My father and mother are reasons for me becoming a lawyer by profession, May God keep them healthily and bless them abundantly.

I will do no better if I don't mention my lovely wife Miriam Edwin who through ought my Master program, she has played a vital role of not only encouraging and taking care of me but also for her prayers, courage and love.

Last but not least, my dedications extend to the following heroes for the reasons best known to me. These are my two biological children Castor Edwin and Jaydan Edwin. My lovely blood brothers; Denice, Auson and Datius.My lovely sisters: Edna, Revina, Valeria, Neria and Gloria.

ACKNOWLEDGEMENT

I thank the almighty God for protecting me throughout my Master programme. I would like in a very special way to express my heartfelt appreciation to my supervisors Dr. Saphy Bullu and Dr. Rindstone Ezekiel for their intellectual guidance throughout the entire period of my Master programme. My sincere gratitude is further extended to my parents for their love and care. I also extend my sincere thanks to my family for their prayers.

In a special way, I thank Victor Robert Mkwavi for his financial support towards accomplishing this work.

Finally, my sincere gratitude is extended to all those who participated in this study including my colleagues for their social and academic support.

ABSTRACT

The rapid evolving digital devices technology give rise to emergency of electronic evidence which in turn poses challenges to traditional rules of evidence notably relevance, hearsay, authentication and best evidence rule. As it has been noted, the rules which were applicable to paper-based evidence are now applicable to electronic evidence. Conversely, the new digital rules of admissibility of electronic evidence which have been enacted in Tanzania, particularly the new specific law; the Electronic Transaction Act,2015 tend to limit the traditional rules in Evidence Act while themselves are insufficient to cater the technological digital demands. It is not clear whether the new digital rules modify the existed ones to be adopted to this current technological reality. The effect renders confusions, inconsistent case laws as well as rendering evidence inadmissible thereby limiting their scope of admissibility and vice versa, which in turn, injustices to the society. This study aims to assess the entire rules of admissibility of electronic evidence in Tanzania and its enactment of digital laws to see if the letters of law are sufficient and ideal to technological reality. To achieve the target, the study employed pure doctrinal legal research methodology which allows scrutiny over the letters of law and makes use of the existing literature to critically analyse and explore challenges of admissibility of electronic evidence. The study disclosed that the current legal situation is not the ideal as legal provisions are insufficient, heterogeneous and primitive when interpreted by courts in the prevailing digital environment. The study finally recommends workable solutions, among others to overhaul entire legal framework for admissibility of electronic evidence and amend the provisions and enact which will modify the existed traditional rules to quench thirsty of current technological environment.

TABLE OF CONTENTS

LIST OF LEGISLATIONS

List of legislations in Tanzania

The Constitution of the United Republic of Tanzania, 1977 (as amended)

Evidence Act (TEA), Cap 6 (R.E 2019)

Electronic Transaction Act (ETA) No.13 of 2015(R.E 2019)

The Cyber Crimes Act (CCA) No.14 of 2015(R.E 2019)

International Instruments

United Nations Convention on the Transnational Organised Crimes (UNTOC)

United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce.

Council of Europe Cybercrime Convention (Budapest Convention),2004

Commonwealth Model law of Electronic Evidence,2017

Draft Convention on Electronic Evidence

Explanatory memorandum notes to electronic Convention

Guidelines and explanatory memorandum on electronic evidence in civil and administrative proceedings adopted by the Committee of Ministers of the Council of Europe on 30 January 2019 and explanatory memorandum.

Electronic Evidence Guide, a basic guide for police officers, prosecutors and judges Version 2.0, Cybercrime Division Directorate General of Human Rights and Rule of Law Strasbourg, France drafted 15 December 2014 funded by European Union and Council of Europe.

List of legislations in other jurisdictions

US Federal Rules of Evidence, printed 2019

UK Criminal Justice Act, 2003

LIST OF CASES

List of Cases in Tanzania

Trust Bank of Tanzania Ltd v. Le Marsh Enterprises Ltd (2002) TLR 144

Emmanuel Godfrey Masonga v Edward Franz Mwalongo Misc. Civil cause no.6 of 2015, HCT (Iringa District Registry) at Njombe, (Unreported).

Joseph Mbui Magori, Laurence Macharia High Court of Tanzania (Commercial Division) at Dar es Salaam Commercial case no. 4 of 2000 (unreported).

Lazarius Mrisho Mafie & Another v Odilo Gasper, Commercial case No.10 of 2008 (Unreported)

Tanzania Cotton Market Board v. Cogecot Cotton Company SA [1997] 165 (CA)

Tanzania Bena Co. Ltd v. Bentash Holdings Ltd, Commercial Case No. 71 of 2002 (Unreported).

Exim Bank (T) Ltd v Kilimanjaro Coffee Company Commercial Case No 29 of 2011 (HC Commercial Division at Dar es salaam) (Unreported)

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

Simbanet Tanzania Limited vs Sahara Media Group Limited Commercial Case no.2 of 2016 The High Court of Tanzania, Commercial Division at Dar es salaam (Unreported)

EAC Logistic Solution Limited vs Falcon Marines Transportation Limited

Civil Appeal No.1 of 2021, High Court of Tanzania at Kigoma (Unreported)

Leonard A. Munghor vs Novart Kaijage Zedekiah Civil Case No.04 of 2021, High Court of Tanzania at Bukoba (Unreported)

Onesmo Nangole vs Dr, steven Lemomo Kiruswa and two others Civil Appeal no. 117 of 2017, CAT at Dar es Salaam, (Unreported)

Ivanna Felix Teri vs Viettel Tanzania Public Limited Company and Another Civil Case no. 7 of 2019, High Court of Tanzania at Moshi (Unreported)

I & M Bank (T) Limited vs Gregory Ogweyo Consolidated Revision no. 724 & 761 of 2019

Kahama Oil Mills Ltd and Another vs Messina(T) Ltd High Court of the United republic of Tanzania (Labour Division) Commercial Case,No. 86 of 2019 HCT Commercial Division at /Dar es Salaam(Unreported)

Ami Tanzania Limited vs Prosper Joseph Msele Civil Appeal No.159 of 2020, CAT at Dar es Salaam (Unreported).

Fadhili Mbwana vs Raymond William Komba DC Civil Appeal No.06 of 2022, HCT at Songea (Unreported)

List of Cases in England

R v Cochrane 6 [1993] Crim LR 48 (CA)

R v Boulkhrif [1999] Crim LR 73 (CA).

R v Mawji (Rizwan) [2003] EWCA Crim 3067, [2003] All ER (D) 285 (Oct)

Re VeeVinhnee, Debtor American Express Travel Related Services Company, Inc v VeeVinhnee 336 BR 437 (9th Cir BAP, December 16, 2006)

Greene v Associated Newspapers [2005] QB 972

List of Cases in United States of America

Armstrong v Executive Office of the President 1 F.3d 1274 (D.C)

Zubulake v UBS Warburg LLC (Zubulake) 1217 F.R.D. 309 (S.N.D.Y, 2003).

Yahoo case

LIST OF ABBREVIATIONS

AC	Appeal Cases
AAL	American Association of Libraries
AU	African Union
CA	Court of Appeal
CD	Compact Disc
CCA	Cyber Crimes Act
CMA	Commission for Mediation and Arbitration
Ch.	Chapter
CJ	Chief Justice
CO	Company
Corp.	Corporation
CURT	Constitution of the United Republic of Tanzania
EAC	East Africa Community
ETA	Electronic Transactions Act
ER	England Report
EU	European Union
EWCA	England and Wales Court of Appeal
F.	Federal reporter
F.2d	Federal reporter Second Series
F.3d	Federal reporter Third Series
FLR	Federal Law Reports
FRD	Federal Rules Decisions
GDRPR	General Data Protection Regulation

HL	House of Lords
ICT	Information Communication Technology
Inc.	Incorporated
IP	Intellectual Property
ISP	Internet Service
J	Judge
KB	Kings Bench
KLR	Kenya Law Reports
LCD	Liquid Crystal Display
LJ	Lord Justice
LLC	Limited Liability Company
Ltd	Limited
MLA	Mutual Legal Assistance
MU	Mzumbe University
OUT	Open University of Tanzania
PLC	Public Limited Company
QB	Queens Bench
RE	Revised Edition
SA	South Africa
S.D.N.Y	Southern District New York
TANZLII	The website based at the Judiciary of Tanzania and publishes the law of Tanzania for free online access.
TEA	The Evidence Act
TLR	Tanzania Law Report

UDSM	University of Dar es Salaam
UELMA	Uniform Electronic Legal Material Act
UK	United Kingdom
UN	United Nations
UNCITRAL	United Nations Convention on International Trade Laws
UNTOC	United Nations Convention against Transnational Organised Crimes
U.S	United States
V	Versus
VCD	Video Compact Disc
WLA	Written Laws miscellaneous Amendments
WLR	Weekly Law Reports
WWW	World Wide Web

CHAPTER ONE

INTRODUCTION AND BACKGROUND TO THE PROBLEM

1.1 Introduction

This chapter portrays the contextual framework of the problem under study. In that regard, it starts with the narrations of the historical background to the problem to trace where the problem originated. It proceeds by stating the statement of Problem of the research. Since there are previous researchers who have dealt with the subject, this chapter conducts the literature review through various scholars and build the gap to justify why the current study is inevitable.

The chapter discloses objectives of the study, both general and specific. The chapter further raises research questions which the current study seeks to offer solutions. It proceeds to explain the significance of the study and the scope of it. Furthermore, the chapter lays out methodologies used to collect data as well as sources where the data is obtained and its limitations. Finally, the chapter explains how the entire dissertation is organised chapter wise.

1.2 Background to the Problem

The general legislation which regulates the admissibility of electronic Evidence in judicial proceedings in Tanzania is The Evidence Act (TEA)[1] The said Act was enacted in 1967 and it therefore repealed the Indian Evidence Act 1872 which had been in force since 1920. The former Indian Evidence Act,1872 was the British model statute introduced to India and later transferred to British colonies including

[1] Evidence Act (TEA) 1967, Cap 6 (R.E 2019), s 2

Tanzania (formally known as Tanganyika).[2] It is ostensibly viewed that the said Indian statute incorporated the English rules and principles of evidence in a modified version to suit the circumstances of India because India was one among British Colony.

Although the Tanzania Evidence Act, 1967 came to replace the Indian Evidence Act 1872, it retained most of the Indian Evidence Act provisions.[3] The Tanzania Evidence Act, 1967 like the former Indian Evidence Act 1872, dates back to before the age of computer technology. The rules and principles incorporated in both of the said statutes were not directly intended to regulate the electronic environment, just as it was a common trend across many jurisdictions in the 1960s including Tanzania.[4] The subsequent period to 1960 the word witnessed the rapid technological revolutions which ultimately our Tanzanian courts were confronted with cases involving admissibility of electronic evidence.[5]

The mushrooming cases on electronic evidence in the courts of Tanzania, necessitated the legislature to amend TEA to include admissibility of electronic Evidence but it retained the codified common law exclusionary rules of admissibility of evidence such as relevance, admissibility, authentication, hearsay, the best evidence and corroboration.[6] Though TEA is a principal legislation but it is not

---

[2] Makulilo, A. B, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review,2007, p.56

[3] The retained provisions include common law rules on admissibility of evidence notably, hearsay, corroboration, relevancy and best evidence rule etc.

[4] Makulilo A.B (n.2),56

[5] For instance, the High court of Tanzania was confronted with the first land mark case of Trust Bank of Tanzania Ltd v. Le Marsh Enterprises Ltd (2002) TLR 144 which was tested on admissibility of electronic evidence before amendment of TEA to include electronic laws.

[6] The amendment came from an alarm of High Court Commercial Divisions on the case of **Trust Bank of Ltd v. Le Marsh Enterprises Ltd (2002) TLR 144**.The Written Laws (Miscellaneous Amendments) Act,2007

exhaustive, in the sense that if there are other legislations which may be enacted for the purpose of specifically regulating certain type of evidence the latter will prevail.

Now, with the advent of global development of technology and the spread of ICTs and Internet penetration in Africa has raised concerns over the need to promote cybersecurity governance and cyber stability in the continent.[7] However, the move to promote cyber security was not only pioneered under regional level in Africa but also under global level, international instruments had had already been enacted. [8] This need prompted the African Union in June, 2014 to establish a regional cybersecurity treaty known as the African Union (AU) Convention on Cyber Security and Personal Data Protection.[9]

The Convention imposes obligations on Member States to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime.[10] It was on this pressure Tanzania enacted two pieces of legislations which are The Cyber Crimes Act[11] and The Electronic Transaction Act (ETA)[12] both of 2015 which compliment Evidence Act to regulate admissibility of electronic evidence.[13]

---

introduced Section 40A,76 and 78A, these changes were made through sections 33,34 and 35 of Written Laws (Miscellaneous Aamendments) Act respectively. Section 40A of TEA deals with admissibility of electronic evidence in criminal proceedings while Sections 76,78A are closely related dealing with admissibility of electronic evidence in civil matters but only in banker's books.

[7] Uchena, J.O, "The African Union Convention on Cybersecurity; A regional response Towards Cyber Stability? Masaryk University Journal of Law and Technology, 2018, Vol.12.2, p.92

[8] See The United Nations Convention on Transnational Organised Crime (UNTOC),2000 which was adopted by the General Assembly on November 15,2000. See also The Council of Europe convention on Cybercrime (the Budapest Convention) opened for signature 23 November,2001 and entered into force 1 July 2004.These are the products of international effort to regulate cybercrimes.

[9] (n.7), 92

[10] ibid,92

[11] Act No.14 of 2015. According to the long title of the Act is an Act to make provisions for criminalizing offences related to computer systems and Information Communications

With the above enacted local electronic statutes which were the results of regional and international Instruments, today for both Civil transactions and Criminal activities captured through the use of Technology, retrieved as electronic evidences from digital devices, are admitted in Tanzanian courts of law. Tanzanian law defines electronic evidence to mean "any data or information stored in electronic form or electronic media or retrieved from a computer system, which can be presented as evidence"[14] Alternatively, electronic evidence is any probative information stored or transmitted in digital form; such information can be stored in computer hard drive, optical disks, floppy disks, remote internet storage, handheld devices, memory cards, network servers, emails etc.[15]

Therefore, on account of the above legal definition, just like traditional evidence, electronic evidence is admissible in Tanzanian courts. Admission is a statement, oral or documentary, which suggests any inference as to the fact in issue or relevant fact and which is made by any of the persons and in the circumstances hereinafter mentioned.[16] The court may as well admit data message which is defined as data generated, communicated, received or stored by electronic, magnetic optical or other

---

Technologies; to provide for investigation, collection, and use of electronic evidence and for matters related therewith.

[12]Act.No.13 of 2015. According to the long title of the Act is an Act to provide for legal recognition of electronic transactions, government services, the use of information and Communication Technologies in collection of evidence, admissibility of electronic evidence, to provide for the facilitation of use of secure electronic signatures, and to provide for related matters.

[13] Also, The African Union Convention on Cyber Security and Personal Data Protection, in June, 2014. (The Malabo Convention) The Convention imposes obligations on Member States to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime.

[14] Electronic Transaction Act (ETA) No.13 of 2015, s. 46(3)

[15] Gultan, G, Privacy Concerns relating to the collection of electronic evidence: under Turkish legal system and cybercrime convention, master's Thesis (n.y), Faculty of Law University of Oslo, p.6

[16] TEA, s. 19

means in computer system or transmission from one computer to another.[17]

Similarly, for purpose of admission, the current version of TEA has therefore embraced the changes over digital technology where document may be in paper or electronic form.[18] Thus, the term document has been defined to mean any writing, handwriting, typewriting, printing, Photostat, photography, computer data and every recording upon any tangible thing, any form of communication or representation including in electronic form by letters, figures, marks or symbols or more than one of these means.[19] Electronic Evidence could be retrieved and printed in hard copies or stored in video LCD during admissibility. In its nature, it is susceptible of being altered or deleted and also it has a challenge of telling the original document. With that ephemeral nature of electronic evidence, the existed traditional rules of admissibility when interpreted with the insufficient enacted digital rules by courts depicts the inconsistences and paradoxes.

1.3 Statement of the Research Problem

The admissibility of electronic evidence in Tanzania faces significant challenges due to its distinct characteristics and the inadequacies of existing legal frameworks. Recent digital laws, including the Electronic Transactions Act (ETA) and the revised Tanzania Evidence Act (TEA), have strained traditional common law rules such as relevance, hearsay, and authenticity. This strain leads to inconsistencies in how courts interpret these laws, resulting in potential injustices. For instance, in *Ivanna Felix Teri vs. Viettel Tanzania Public Limited Company*,[20] the High Court insisted on

[17] ETA, s. 3
[18] ETA, s.3
[19] Evidence Act, s 3 (as amended by The Written Laws (Miscellaneous Amendments) Act, 2007)
[20] Civil Case No.7 of 2019,High Court of Tanzania at Moshi(Unreported)

the original photo to validate an Instagram image, undermining the value of digital evidence.

The legal concept of authenticity remains tied to traditional notions of original evidence, which do not align with the realities of electronic documentation. Section 18 of the ETA, which aims to facilitate the admissibility of electronic evidence, paradoxically coexists with TEA's common law principles, causing further confusion. The amendments in the TEA and the ETA lack comprehensive safeguards for ensuring the uniform authenticity of electronic evidence, leading to varied judicial outcomes.

Notable cases, such as *Exim Bank (T) Ltd v. Kilimanjaro Coffee Company*[21] and *EAS Logistic Solution Ltd vs. Falcon Marines Transportations Limited*,[22] highlight conflicting judicial interpretations regarding the necessity of certificates and affidavits for electronic evidence. These discrepancies exemplify the inadequacies in the legal framework, particularly the absence of established procedures for authenticating electronic records. Moreover, the Court of Appeal of Tanzania has not definitively resolved these inconsistencies, leaving lower courts to grapple with conflicting precedents.

As it stands, the current legal regime appears to lack cohesive rules for the authentication of electronic evidence, resulting in ongoing uncertainties that could affect both civil and criminal proceedings, especially in light of recent cybercrime legislation. Without a robust and coherent legal framework, the potential for injustice

[21] Commercial Case No.29 of 2011(HC Commercial Division at Dar es Salaam)(Unreported).
[22] Civil Appeal No.1 of 2021,The High Court of Tanzania at Bukoba(Unreported)

remains high, underscoring the urgent need for legal reform to address these challenges.

1.4 Literature Review

There is a good number of scholars in Tanzania and others from foreign jurisdictions who have written on the issue of admissibility of electronic evidence but in different contexts depending on the particular aspects they are referring to at the given particular time. However, the issue of admissibility of electronic evidence is borne out by the emergency of development in technology which differs from one country to another, the available literature will also differ from the current study in terms of time/era, aspects, scope, basis, prevailing law and jurisdiction. The following literatures are reviewed to justify the undertaking of the intended study:

Makulilo,[23] categorically wrote on the admissibility of computer evidence in Tanzania. Makulilo therefore discussed the Evidence Act,[24] in connection with case laws drawn from Tanzania and other common law jurisdictions relevant to the issue of admissibility of electronic evidence retrieved from the computer as electronic document. Makulilo therefore observed that TEA had problems of lagging behind the digital era due to the fact that the law was enacted without contemplation of digital environment. Having critically examined the provisions of TEA in its entirety the said author also found that at that particular time there was no meaning on the term of electronic document under TEA the only definition which was available was that of the document which excludes the concept of an electronic document. In his

[23] Makulilo, A.B., *Admissibility of Computer Evidence in Tanzania*, Digital Evidence and Electronic Signature Law Review,2007

[24] Cap 6 (now R.E 2019)

research, the author concluded by discussing the challenges facing courts in telling the difference between original and copy in computer evidence. Makulilo therefore called for reforms. It is also worth noting that Makulilo's research was limited to computer evidence and not any other types of electronic evidence retrieved in any electronic device which this study seeks to canvas.

Makulilo.,[25] subsequently conducted another research whereby he dealt with the admissibility of electronic evidence in Tanzania to see if the new rules have been applied consistently by courts through case laws. This was research after amendment of TEA and enactment of ETA. Makulilo managed to analyse the case law prior to and after amendment and finally found that there were uncertainties as to evidentially issues of electronic evidence. Makulilo further discovered that it is not clear to what extent the exclusionary common law rules of admissibility of evidence namely relevancy, authenticity, hearsay and best evidence rule codified in TEA apply in the context of electronic evidence. The author therefore suggested that the effect of the amendments brought about by the Written Laws (Miscellaneous Amendments) Act 2007 to TEA as well as ETA in admissibility of electronic evidence in criminal and civil cases needs thorough assessment.

The author also observed that it is difficult to determine the extent the new rules in Written Laws miscellaneous Amendments (WLA) on ETA modify the existing common law rules of Evidence. Furthermore, the said author was certain that the new rules in ETA are insufficient. Makulilo tried to critically analyse the existing

[25] Makulilo A.B, *The admissibility of electronic evidence in Tanzania: new rules and case law*, Digital evidence and Electronic Signature Law Review,13,2016.

digital laws of admissibility of electronic evidence and challenges of digital era. This literature is significantly palatable to issues of admissibility of electronic evidence. It is ranked as ground's work of the intended research but a vital point of departure is the scope and thus it did not offer the real solutions to the researcher's identified problem rather than calling for a thorough assessment neither does it have a tested result on laws visa vi practice which is the domain of this research's objective. It does not offer the manner and extent how the digital rules should be enacted to solve the problem. The current research intends to cover such aspect.

Tegamaisho[26] in a close relation with the above reviewed Makulilo's articles, titled "Authenticity of Electronic Evidence; A comparative analysis between the Position in Tanzania and Kenya" The author made a comparative analysis between the position in Tanzania and Kenya. The author observed that in Tanzania, courts for quite long time have been relying on common law doctrine of best evidence Rule to which the primary evidence in most cases is written and signed on authenticated documents. That the challenges now facing the court are the use of electronic evidences in courts. The said author cemented that the same challenge is posed in the law of evidence since it does not cover electronic evidence such as data stored or transmitted using a computer.

Tegamaisho criticized the amendments effected in TEA in 2007 as it did not address the issue of authentication of electronic evidence. Tegamaisho therefore analysed the issue of authentication of electronic evidence in Tanzania by drawing a comparative

[26] Tegamaisho P.P, *Authenticity of Electronic Evidence; A comparative analysis between the Position in Tanzania and Kenya*, Ruaha Law Review Faculty of Law Ruaha Catholic University,2018, Vol.5-6y, No.1

analysis from Kenya as Kenyan evidence law provides the modes in which electronic evidence can be authenticated. He therefore found that Kenyan law has conditions that need to be fulfilled when admitting electronic evidence. Tegamaisho therefore suggested Tanzania to follow the footsteps in Kenya in authenticating electronic evidence. This literature has great input in admissibility of electronic evidence but limited only to issues of authentication.

Tegamaisho stickled his critique only on TEA and its amendments of 2007 in his article published in 2017-2018 journal while the Electronic and Transaction Act was already in force as it was enacted in 2015 but his research is devoid of literature touching on the digital rules enacted in ETA which is also a concern in this current study. Besides, Tegamaisho's research was limited to authentication rule only and no other rules of admissibility of evidence and therefore could act as the take off point of the intended study so as to further investigate on other digital rules of admissibility of electronic evidence in broader perspective.

Mambi.,[27] similarly explains the status of admissibility of electronic documents under the legal system in Tanzania in light of the Land mark case of *Trust Bank Tanzania Ltd vs Le-Marsh Enterprises Ltd,(Supra), Joseph Mbui Magori, Laurence Macharia*[28] case laws where the said scholar noted that digital evidence requires proper forensic investigation to identify, extract, preserve and document digital evidence. Mambi concluded that the changes in Tanzania legal system are not

[27] Mambi, A.J, *Electronic evidence in Tanzania*, Digital evidence and Electronic Signature Law Review, 2013, Vol.10

[28] High Court of Tanzania (Commercial Division) at Dar es Salaam Commercial case no. 4 of 2000 (unreported)

sufficient. The reviewed work supports the researcher that there is still a need to carry on lucid investigation which will encompass practical aspect in field to curb the insufficiency of legal regime which the literature observed.Moreover,the literature do not encompass the enactments of provisions of ETA introduced in 2015 as the scholar had investigated back before where the material available at that time could not have solved this author's problem in current situation.

Ubena.,[29] in similar context with Mambi's above reviewed literature, wrote on tendering and admissibility of electronic evidence in Tanzania. Ubena guided that when computer printout is tendered before the court of law as evidence certain Important features of data message such as the meta data may be missing or become invisible as they cannot be printed out. The author therefore noted that assurance of data message's reliability becomes crucial. The challenge though is how to prove reliability and authenticity of data message. Ubena therefore found that reliability and authenticity may be achieved by laying down the foundation of the data message. Ubena noted the solution to be crucial because of the ephemeral nature of electronic evidence.

The scholar suggested that laying foundation to establish authenticity of electronic evidence may involve a computer forensic expert. In this reviewed literature emphasis was on the ephemeral nature of electronic evidence towards laying foundation to ascertain its reliability and authenticity, it therefore paves way to investigate further and come up with solid approaches on what rules and principles

[29] Ubena.J., Guiding notes on tendering and admissibility of electronic evidence in Tanzania,1st Ed, Tanganyika Law Society, Dar es salaam,2020

should be adopted to minimise or remove the paradoxes in the admissibility of electronic evidences in our legal system which is devoid of the current literature.

Ubena.,[30] consistently, again in another study wrote on the legal issues surrounding the admissibility of electronic evidence in Tanzania where he examined the amendment in TEA and enactment of ETA laws which came to cater admissibility of electronic evidence and hence, he found that despite the available legal frame work there is still a risk of unreliable evidence being admitted. The author further found that the courts also seem to have applied the laws inconsistently. The author therefore called for reforms. The literature is palatable in admissibility of electronic evidence but in different aspect, context and scope as touched nothing concerning the paradoxes in Tanzanian courts especially on the law vis vi practice though its input is therefore the ground work of the intended study.

Liu.,[31] Similarly wrote on the problems on the admissibility of electronic evidence in the Chinese context where he analysed the pitfalls caused by the requirement of submitting electronic evidence in courts with preference of original evidence and therefore found that in Chinese judicial practice there is a rigorous standard of admissibility for electronic evidence. But also found that there are other challenges such as misunderstanding between admissibility and probative value (weight of evidence) where important electronic evidence may be neglected for its admissibility simply because it is capable of being tempered or altered which is the criterion for

[30] Ubena.J, *Legal issues surrounding the admissibility of electronic evidence in Tanzania*, Digital Evidence and Electronic signature Law Review,2021, Vol No.18,66

[31] Liu.B., *Problems on the admissibility of electronic evidence in the Chinese Context*, Digital Evidence and Electronic Signature Law Review,2015,12

weight of evidence and probative value but not admissibility. Liu also found the challenge of lack of knowledge on electronic evidence and lack of authentication procedure in Evidence law in China.

Liu reasoned that since the requirement of need for original in physical item is emphasized which imposes strict restriction on admissibility rules of electronic evidence which can subsequently lead to substantial justice, especially in the fraud cases and since the rules do not come into play after the evidence is introduced to court, Liu was therefore of the view that the rules of exclusion should start from collection and discovery process. The literature is of vital aid in comparison and lessons to draw from but since it was conducted in China hence the veil between it and this study lies on jurisdiction divergence.

Osinbajo.,[32] similarly researched on the Nigerian Law of Evidence where the author marked that it was slow in recognising the challenges of proof of electronically generated evidence. Osinbajo explained that the Evidence Act of Nigeria,1945 was only amended to recognise Electronic Evidence in 2011.Osinbajo finally found that the courts had always taken a proactive view despite the constraints of the law. The gist from this literature is to show the inevitability and necessity of reforms to traditional rules of evidence which have been done in Nigeria. Being the foreign jurisdiction study carried in Nigeria it therefore bolsters the inevitability of conducting the similar investigation in Tanzania.

[32] Osinbajo, Y.S, Gathering and Admissibility of electronically generated evidence

Thomson.,[33] wrote on the new challenges on admissibility of electronic evidence in Mobile devices in American courts. The legal scholar observed that the widespread use of mobile devices has created unprecedented challenges in legal proceedings as the courts decide how to properly authenticate digital information under the current judicial rules and procedures. Thomson further critically observed that although the basic legal requirements for establishing a foundation for admissibility of evidence in US courts are well -established but the applicability to digital data and devices from which electronic evidence is generated raises many difficult evidentiary issues and questions. As a result, the scholar found that courts have applied widely different standards for similar types of evidence when computer generated information and digital images are presented in courts.

Thomson presents that in order any evidence is admissible it must be authenticated. The said scholar therefore observed that the requirement means that data and information in digital form must be shown to be what the proponent claims that it is. Thomson therefore cemented that the foundations for digital evidence are based on the long-established traditional principles of authentication and admissibility that originated with the use of paper-based evidence of relevance, Authenticity, hearsay, best evidence and probative value which in digital reality brings prejudicial effect.

Thomson therefore found further that the traditional foundation for electronic evidence which US courts have been admitting computer records in to evidence since the 1970s when computer systems became available for business and personal

[33] Thomson, L.L, *Mobile Devices, New challenges for Admissibility of Electronic Evidence*, SciTech Lawyer,2013, Vol 9.3

use which focused on the relationship between the information and computer where documents were admitted basing of the assumption that the information produced from the computer is inherently reliable but now the nature of digital evidence is significantly different from that early days of mainframe stand- alone computer records. Thomson therefore finally gathered that, the traditional foundations for computer record may no longer be adequate to address the complexities of modern information system from which electronic evidence is generated because digital information may be created easily and without any verifiable record of who did so, and it can be changed often without detection.

The said legal scholar therefore suggested reforms of laws and that deeper knowledge of understanding electronic evidence is required. The literature is of great assistance in terms of admissibility of electronic evidence in mobile devices and its challenges which may help the researcher to draw lessons from foreign jurisdiction but its approaches which stemmed from pure doctrinal theories and concepts cannot real suit to our local circumstances in Tanzania as it was conducted in USA hence the need to carry the study in Tanzania under practical perspective.

Swales.,[34] carried a study and published on the regulatory environment governing Hearsay electronic evidence in South Africa where the said author examined and considered the definition of data message in the context of hearsay electronic evidence and concluded that the amendment is required. Swales concurred with the suggestions of the South Africa Law Reform Commission that data message can

[34] Swales. L, *An analysis of the Regulatory environment governing Hearsay Electronic Evidence in South Africa: Suggestions for reforms*, Part two PER/PELJ,2018 Vol.21-DOI

constitute hearsay within the meaning of the applicable legislation. Swales further suggested that South Africa law must distinguish between data message produced substantially by a computer or mechanical process and those substantially on the credibility of the person. The literature greatly contributed on the definition of data message but the research being conducted in South Africa it stimulates an investigation to be undertaken in Tanzania.

Teppler.,[35] similarly, wrote on the issue of digital data as hearsay. This scholar examined the proposition that all digital data is hearsay in legal proceedings within the United States of America. Teppler analysed the inadequacy, if not outright failure, of the current approaches to dealing with the hearsay exception used to offer computer generated information into evidence. Teppler observed that there is no uniformity of approach in lower court decisions towards the issue of authentication and admissibility of computer-generated information offered as evidence in trial. That no guiding rules in courts as to whether digital data is inadmissible hearsay or not. Teppler further observed that some judges consider it inadmissible and others admit it under exceptions of hearsay which apply to traditional evidence.

The author proposes that until the Federal Rules of Evidence are revised to reflect the ephemeral nature of digital evidence, such evidence should be considered hearsay and deemed inadmissible unless a hearsay exclusionary exception is successfully asserted. Teppler further proposed that if admissibility of digital evidence is sought pursuant to a hearsay exception, such evidence should be made

[35] Teppler, S.W, *Digital Data as Hearsay*, Digital Evidence and Electronic Signature Law Review,2009, Vol 6,7

subject to heightened reliability requirements. This literature needs appraisal as it acknowledges the challenge on the rule of hearsay being affected by the digital environment which is one of the rules this research seeks to investigate in Tanzania where rules are quite different from federal rules and coming up with solid approaches which fits to local circumstances.

Teppler,[36] in another closely related study, writes on the testable reliability in the modernised approach of admissibility of electronic evidence. The said author examined the proposition that all digital data sought to be introduced and admitted as evidence should be subject to a heightened showing of reliability and testability. Teppler found this objective could be reached by either: (1) considering all digital data as hearsay pursuant to Federal Rule of Evidence. (2) creating a new evidence rule requiring such a showing as a predicate to admissibility; or (3) the emergence of express decisional authority.

In his literature Teppler also analysed the inadequacy of the current approaches to dealing with the hearsay exception used to offer computer- generated information into evidence. The scholar proposed that until the Federal rules of Evidence are revised to reflect the highly mutable and untestable nature of digital evidence, such evidence should be treated as hearsay and subject to application of existing traditional rules on hearsay which deemed hearsay inadmissible unless an affirmative showing of reliability and testability is successfully asserted. It is the vital literature in appreciating the challenges in admissibility of digital evidence but

[36] Teppler, S.W, *Testable reliability; Modernised approach to ESI admissibility*, Ave Maria Law Review,2014, Vol.12

conducted in different jurisdiction from the intended research and hence the inevitability of this study in Tanzania. Crossey,[37] in connection with admissibility of evidence generated from a computer, writes on the rule of hearsay in relation to Machine Translator Testimony and the confrontation Clause in Federal Rules to see if the time has come for the hearsay rule to escape from the stone age.

In his work, Crossey noted that the use of machine translator can either facilitate or impede the ability of non-English-speaking witnesses, suspects and defendants to understand and exercise their constitutional rights. He found that many scholars and courts have disagreed whether a non-English -speaking defendant's translated statements can be used against him or her without opportunity to cross examine the translator. He also found that scholars and courts have also wrestled with whether machines are declarants and subject to confrontation.

Crossey finally concluded that the noted gap bridges the unsettled issues of law and therefore focused on the potential problem that the federal Rules of Evidence do not address whether the confrontation clause in their amendments in law affords the defendant the right to confront this machine generated testimony. The author finally suggested amendments on hearsay rule as machine translation poses an increased risk of error while confrontation clause's purpose was to establish that evidence is reliable. The literature is worth to receive appraisal in evidence generated to translation machine which is peculiar aspect and in different scope from what the intended research views in Tanzania.

[37] Crossey, N.E, *Machine Translator Testimony & the confrontation Clause: Has the time come for hearsay rule to escape from the stone age?* Drexel Law Review,2020, Vol.12,561

Tejas, Anand and Dhawan[38] carried the similar study and published on the admissibility of electronic evidence in line with how Supreme court of India re-defined their rules. The co- authors narrated that the emergency of digital era has provided the much-required impetus to the appreciation of digital evidence. Therefore, India keeping with the time, the requisite amendments were introduced to the Indian laws in the year 2000 with the introduction of Information Technology Act, 2000 which brought the corresponding amendments in Indian statutes including the Evidence Act, 1879. The said authors cement that Evidence Act has been amended from time to time to provide for the admissibility of electronic records.

The Scholars discovered that new provisions for mandatory authentication and reliability of electronic evidence have been put in place. The scholars found that despite of the efforts of the law keeping pace with technology, the lower judiciary in India are technologically unreliable as they do not appreciate the authenticity issues or ensure safeguards while allowing the admissibility of electronic evidence. They finally suggested the law makers the need for additional safeguard for the court to adopt a consistent approach on authenticity, integrity and reliability in view of admissibility of electronic evidence. The literature shades on the digital rules of reliability and authenticity in India. However, it does not come with the solid answers suiting to Tanzania situation whether we need to re-write new rules for admissibility of electronic evidence which is in domain of the intended researcher's scope. Since also the literature is limited in India, the intended research entails to investigate the Tanzania situation.

[38] Anand, A et al, *The Supreme Court of India re-defines admissibility of electronic evidence in India*, Digital Evidence and Electronic Signature Law Review,2015,12

Stanfield,[39] wrote on authentication of electronic evidence in Australia where he analysed the existing rules of evidence in Australia starting from discovery/disclosure of electronic evidence and found some traditional rules for instance estoppel, parole, best evidence, hearsay and their exceptions are not ideal to the contemporary times of digitization when they are strictly applied without modification. Stanfield found that from that gap there are inconsistent applications by courts to authentication of electronic evidence.

The scholar further noted that the entire process of processing, reviewing, and analysing of electronic evidence needs knowledge and expertise in technology so that the presentation to court at the trial for admission otherwise may yield feeble results. It is not worthless to cement that the literature supports the intended study on pertinent issues of rules of collecting, storing and generating electronic evidence and its ephemeral nature for presentation to courts. Nevertheless, where it ends is where this current study entails to take off investigating the paradoxes in courts and however it reveals the practice in Australia centrally to the intended study in Tanzania.

Mason,[40] similarly investigated on electronic evidence and touched on issues of admissibility, authentication and integrity of electronic evidence. Mason noted that traditional normal rules that have developed with respect to the authentication of (mainly) on paper-based evidence are being applied in electronic evidence but

[39] Stanfield, A.R, The authentication of electronic evidence, PHD thesis, Faculty of law Queensland University of Technology, Australia,2016

[40] Mason, S and Seng, electronic Evidence 4th edn,2017

electronic evidence has very different characteristics to paper evidence. The author argued that the rules established for paper no longer apply. That with its unique characteristics and ephemeral nature, complex questions about the integrity and security of electronic evidence rose which must be examined when considering how to authenticate electronic evidence and therefore reforms are inevitable. It is the literature of great assistance in understanding the characteristics and nature of electronic evidence and distinguished from paper-based evidence. However, the points of divergence are that it was conducted in different jurisdiction hence its findings might differ from the intended research but also the scope as it did not go further to investigates the practice of courts and the current study specifically hinges on Tanzanian courts.

Mason.,[41] in similar manner but in different study of electronic evidence and the meaning of original after his study he found that the concept of original cannot be found in digital object in whatever form it takes. That it is necessary to reconsider the conceptual frame work which many lawyers have failed to do. Mason further discovered that the nearest we can get to the concept of an original in digital object is to recognise that it is necessary to consider how authentic the digital object is. That (a) The content of the data that a party relies upon has not changed from the moment it was created to the moment it was submitted as evidence. (b)The data can be proven to be from the purported source(c)The technical and organisational evidence demonstrates the integrity of the data is trustworthy and is therefore considered reliable.

[41] Mason, E*lectronic evidence and the meaning of original*, Amicus Curie 79 Autumn,2 009

Mason therefore calls for reforms to receive the current digital development. The literature is useful in explaining how authentication of electronic evidence should be carried. Nonetheless, its usefulness is limited in only paving a way to the current study to have a starting point where it ends. The intended study will go beyond to see what are better rules to re-write to solve the problems of admissibility of electronic evidence in Tanzania perspective.

Kulehile,[42] dealt with the issues on the regulatory principles of functional equivalency and technology neutrality in the context of electronic signatures in the formation of electronic transactions in Lesotho and SADC region. Kulehile found that the purpose of signature formality is to promote certainty, prevent fraud and provide electronic evidence of a contract. Although found the rules not perfect and ideal as the rules that align with them promote functional equivalence of legal treatment between offline and online signatures. He also found that the reliability and authentication of electronic signature is the question of evidence as is the case in offline contracts. He suggested for soft rules on electronic evidence to compliment electronic signature rules to ensure legal treatment of signatures. The literature has a vital contribution in removing fraud in electronic signature in contracts since electronic signature of an electronic document helps to authenticate the electronic evidence during admissibility.

1.5 Research Objectives

The research Objectives have been categorised into two groups. These are general

[42] Kulehile.M. Analysis of the regulatory principles of functional equivalence and technology neutrality in the context of electronic signatures in the formation of electronic transactions in Lesotho and SADC region, a PHD thesis, Department of Private Law, University of Cape Town, August, South Africa,2017

and specific objectives.

1.5.1 General Objective

This study aims to assess the entire rules of admissibility of electronic evidence in Tanzania and its enactment.

1.5.2 Specific Objectives

This part anticipates undertaking the following:

i. To expose the challenges and problems posed by the admissibility of electronic evidence in the Tanzania legal system in the digital environment.
ii. To assess if the available rules of admissibility of electronic evidence in the Tanzania legal system are in line with the set international standards and other better laws from various jurisdictions.

1.6 Research Questions

This research intends to answer the following questions:

i. What are the challenges of the admissibility of electronic evidence in the Tanzania legal system in the digital environment?
ii. Are the existing rules of admissibility of electronic evidence in Tanzania in line with the set international standards and other better laws from various jurisdictions?

1.7 Significance of the Research

The research study is academic one and therefore useful to academicians, scholars, researchers and legal practitioners at large. Nonetheless, this research is beyond for academic purpose as it will therefore create awareness to various lawyers and

particularly judicial stake holders such as Magistrates, Judges, Advocates, state attorneys, investigators, prosecutors and all other legal practitioners on issues of knowledge pertaining collection, preserving and presentation of electronic evidence as well as the rules of admissibility of electronic evidence. Moreover, the research will help to sensitize the policy and law makers on the need to have reforms on rules of admissibility of electronic evidence enacted so as to quench the thirsty to this current technological reality.

1.8 Research Methodology and Sources

This study employs a pure doctrinal legal research methodology, which focuses on the analysis of existing legal texts and their interpretations. This approach facilitates the examination of both primary and secondary sources to understand the admissibility of electronic evidence within the Tanzanian legal framework.

1.8.1 Research Approach

The research utilizes a qualitative approach, primarily concentrating on doctrinal analysis. This involves critical engagement with legal texts, including statutes, case law, and international instruments, to assess how well existing rules address the challenges posed by electronic evidence in a digital environment

1.8.2 Research Design

The research design is predominantly analytical and applied. Under the analytical framework, the researcher evaluates whether current admissibility rules align with international standards and effectively address existing challenges. The applied perspective involves a critical examination of how these rules interact with

technological advancements and whether they provide adequate solutions to emerging issues.

1.8.3 Data Collection Methods

Data was collected from a variety of primary and secondary sources. Primary sources include legislations which are relevant laws pertaining to electronic evidence, such as the Electronic Transactions Act and the Tanzania Evidence Act and Cyber Crimes Act together with case law which are judicial decisions that interpret and apply these laws in the context of electronic evidence.

For secondary sources include books and journal articles which are Scholarly analyses and discussions that provide context and critique on the admissibility of electronic evidence. Government reports and policies which are documents outlining official positions and frameworks regarding digital evidence. Moreover, regional and international instruments such as the Commonwealth Model Law on Electronic Evidence, which offers a framework for member states. Dissertations and theses were reviewed which are academic works that explore related challenges and potential solutions. Finally, internet resources including online databases and repositories that provide access to legal materials and research.

1.8.4 Sample and Sample Size

The study does not rely on a traditional sample size but instead conducts a comprehensive review of pertinent legal texts and case law. This includes a selection of landmark cases and relevant legislation to provide a thorough analysis of the existing legal framework regarding electronic evidence.

Data Analysis Techniques

The analysis of the collected data involves:

Critical Legal Analysis: This included the evaluating the coherence and applicability of laws concerning electronic evidence. Though the study did not employ comparative methodology but critically analysed by investigating how legal frameworks in jurisdictions such as the USA and UK through the available literature address similar challenges, identifying trends and best practices that Tanzania could consider adopting.

Thematic Analysis: This is done by organizing findings into key themes that emerge from the literature and case law, which reflect the challenges and opportunities in the current legal landscape. The researcher utilized various resources, including online libraries from the Open University of Tanzania, the University of Dar es Salaam, and Mzumbe University, to gather relevant materials. The study also involved accessing online legal databases, including the Tanzanian Judiciary's TANZIIL system. Through this methodological framework, the research aims to critically analyse the rules surrounding the admissibility of electronic evidence and identify gaps and inconsistencies within the Tanzanian legal context, ultimately providing recommendations for legal reform.

1.9 Scope of the Study

The study was delimited to only rules of admissibility of electronic evidence under TEA and those enacted under ETA as well as some of the cases decided after enactment of rules of admissibility of electronic evidence in Tanzania legal system.

1.10 Limitation of the Study

The researcher was not able to discuss all decided cases on digital evidence and rules of electronic evidence in Tanzania as they are many taking into account of the limited resources and time due to costs associated with the nature of doctrinal method deployed. Besides, empirical method was not deployed due to the nature of the study being a fit one to doctrinal method but also the researcher was not able to interview legal practitioners in Tanzania due to the limited time and resources. Moreso, not all legal practitioners are experts in Law of Evidence and ICT laws.

1.11 Organisation of the Study

The study is outlined and organised into five chapters; where in chapter one is the contextual framework of the problem which is the current proposal. In chapter two is the origin and concept of electronic evidence, and definitions to issues pertaining to it. Chapter three covered on the Tanzania legal framework on the law of admissibility of electronic evidence. In Chapter four, the researcher exposes and explores the challenges of admissibility of electronic evidence in Tanzania in the digital environment through case laws and scholarly works. Chapter five is for findings of the study. Chapter six is for recommendation and conclusion. Besides, each chapter has its own conclusion to disclose the insights gattered from the study.

CHAPTER TWO

CONCEPTUAL AND THEORETICAL FRAMEWORK ON ELECTRONIC EVIDENCE

2.1 Introduction

It was portrayed in the previous chapter that the Evidence Act was born out from the Indian Evidence Act which was enacted under colonial legislation in the Indian Subcontinent many years ago. But still today it has remained most significant tool in ensuring dispensation of justice. However, technology has now become a need and human dependency as it has dominated a cyber space due to its fast evolution and rapid growth. Worthless to say, Science and technology are both blessings and disguise because it is the said technology which contributes and facilitates in committing crimes since most of the crimes are committed in cyberspace by utilizing computer and digital technologies. It is on this note that it becomes more important than ever, in this technological era, to emphasize the use of digital evidence in our legal system as a useful tool in order to solve real-world problems.

Thus, considering the issue, this chapter generally provides the definition and conceptual understanding of the term digital technology, electronic/digital evidence. It explores characteristics of electronic evidence. It further explains the types of evidence and difference between traditional evidence and electronic evidence. It defines and explains the common law rules of admissibility traditionally used in evidence with their theories underlying them.

2.2 The Concept of Digital Technology in Electronic Evidence

Digital technology is one of the types of technologies which refers tools, systems

and devices that can generate, create, store or process data. The data processing and logic capabilities of digital technologies are enabled through microprocesses that are programmed to perform various functions.[43] Information technology has caused a paradigm shift in the way individuals and organizations communicate and create, collect, share, and store data and information. Observers on the scene can now document the details of events with photographs, video, and audio recordings from their digital devices such as cell phones and cameras, and postings of real time commentary (often transmitted through their mobile devices) on websites such as YouTube, email, global social media sites, such as Twitter(X), Instagram, WhatsApp etc. and text messages. By so doing the digital/electronic evidence is being collected by use of technological devices.

2.2.1 The concept on Electronic Evidence

In order to understand clearly what electronic evidence entails, it is necessary to know the term ‘evidence’ and ‘electronic’. The term ‘evidence’ means information that is given by a witness whether orally or in writing before the court of law in proving or disapproving certain facts at hand.[44] While “electronic” means accessed by means of computer or any other device. Therefore, Electronic evidence is any probative information stored or transmitted in digital form; such information can be stored in computer hard drive, optical disks, floppy disks, remote internet storage, handheld devices, memory cards, network servers, emails etc.[45]

[43]https://digitalchild.org.au/defining-digitaltechnology Accessed at 23:54,26/08/2024
[44] Tegamaisho, (n.26),2
[45] Gultan, G, Privacy Concerns relating to the collection of electronic evidence: under Turkish legal system and cybercrime convention, Master Thesis (n.y), Faculty of Law University of Oslo, p.6

In other words, Electronic Evidence is any fact in electronic form. It is data message i.e., image, text, audio, or video that may be produced before the court of law to prove or disapprove fact in issue.[46] Electronic evidence is therefore regarded as documentary Evidence.[47] It is therefore important to explain the term document, electronic document and documentary evidence as they are related to electronic evidence.

2.2.4 The concept of Electronic Document

Refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored processed, retrieved or produced electronically. It includes digitally signed documents and any printout or output, readable by sight or other means, which accurately reflects the electronic data message or electronic document. The term "electronic document" may be used interchangeably with electronic data message.[48]

2.3 Application of Common Law Rules of Evidence to electronic evidence

The laws on admissibility of evidence enacted in current legislations have their origin which is traced back from laws of England to wit "common law rules of evidence". The said rules were enacted in Indian sub-continent under British administration. When England extended its colonial administration in Some of

[46] Ubena Guiding notes on tendering and admissibility of electronic evidence, (n.29), 11
[47] Ibid
[48] Mkandya, B.H, Admissibility of Electronic Evidence in Tanzania: Law and Practice, A LLM Thesis, Open University of Tanzania,2011, p 31

African Countries, Tanzania was no exception as it was one of the British Colony, thus the Evidence Act of Tanzania was the result of Indian Evidence Act and most of the provisions are Pari Materia. These common law rules of evidence, despite being enacted long time ago are still applicable today. Some of these common law rules which appear to be relevant and recurring in day-to-day application in our judicial systems are as follows:

> *The Best Evidence rule, Relevance evidence rule, Reliability of evidence rule, Authenticity of evidence Rule, Hearsay Evidence rule and Originality of evidence rule.*

2.3.1 The Best Evidence Rule

This is the common law position, "the Best Evidence Rule". That no evidence is admissible unless it is the best that the nature of the case will allow [49] The Best Evidence rule requires the original document to be produced unless it is not available due to some circumstances like maybe it is destroyed then its copy will be acceptable.[50] Therefore, the rule favours the production of original document to be produced so as to assure the court that there are no alterations made in the document. In addition to that, Nemeth Charles said that:

> *"The Best Evidence Rule derives its support from the conventional wisdom that originals are more reliable than duplicates. Alterations or other modifications are more difficult in original material since it is the most convincing evidence available*". [51]

The origins of this rule date back to the 1800s and it first originated in 18th century British Law and further developed in the case of Omychund vs Barker[52] where Lord Hardwicke remarked that "there is but one general rule of evidence, the best that

[49] Tegamaisho (n.26) ,8
[50] ibid
[51] ibid
[52] [1780] [1744]125ER 1310, [1744] Willes 538

nature of the case will allow"[53] However, in the advent of technology, precisely in electronic communications, it is questioned whether the rule is still valid.

2.3.2 Reliability of Evidence Rule

According to Oxford Leaners Dictionary" Reliability is the quality of being trustworthy, or quality of being likely to be correct or true. It is a circumstantial guarantee of trustworthiness.[54] Some scholars have suggested reliability should be the primary criterion for admitting electronic evidence.[55] In Tanzania, criterions for determining admissibility of data message into evidence are set out under the law, which includes reliability of the manner the data message was generated, stored or communicated.[56]

2.3.3 Authenticity of Evidence Rule

According to Cambridge English Dictionary Authenticity is the quality of being real.[57] Therefore reliability, authenticity (authentication) and admissibility of data message into evidence are crucial issue in the world of electronic communications. Authenticity is like genuineness, credibility or believability. Under Electronic Transactions Act of Tanzania[58] there is a presumption of authenticity of electronic records. But in certain instance authenticity may be hard to achieve without involvement of computer forensic experts.[59]

---

[53] (n.26),7
[54] Ubena, Guiding notes on tendering and admissibility of electronic evidence, (n.29),12-13
[55] ibid
[56] ETA, s 18(2).]
[57] Ubena Guiding notes on tendering and admissibility of electronic evidence, (n.29),13
[58] ETA, s 18(3)
[59] Ubena, Guiding notes on tendering and admissibility of electronic evidence (n.29),13

2.3.4 Relevancy of Evidence Rule

Relevancy relates to admissibility.[60] The general rule is that if the fact applies to the fact in issue, the court will admit it.[61] To determine that the fact is relevant is a process involving both the party who tenders the evidence and the court. The party tendering the electronic evidence must ensure that the evidence is relevant. However, relevancy and admissibility of electronic evidence is not straightforward. Section 18(2) of ETA provides criteria for determining admissibility of electronic evidence.

2.3.5 Hearsay Evidence Rule

Hearsay is defined as a 'statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.[62] A statement is defined in part as an oral or written assertion intended to be an assertion.[63] A declarant is defined as a person who makes a statement.[64] In other words, Hearsay is defined as a statement offered in evidence to prove the truth of the matter asserted.[65]

Therefore, hearsay evidence is the statement that is given by the third party other than declaring in proving certain matter before the court. The rule entails that, "hearsay evidence is not admissible unless there is a showing of substantial reliability of the out of court statement can be assumed.[66] Electronic evidence in its nature may be regarded as hearsay evidence[67] hence, in determining whether

[60] Gultan (n 15),11
[61] TEA, s 7
[62] Teppler, Digital data as hearsay (n.35),13
[63] ibid
[64] ibid
[65] Gultan (n.15),11
[66] Ibid, p.11
[67] Teppler, Digital data as hearsay (n.35),13

electronic evidence is hearsay evidence or not, the distinction between computer generated and computer- stored electronic evidence has to be made.[68]

2.3.6 Primary Document (Original) Rule as Opposed to Secondary Document (Copy) Rule

Primary evidence means the document itself produced for the inspection of the Court.[69] Whereas Secondary evidence includes a certified copies, copies made from the original by mechanical process which in themselves ensure the accuracy of the copy and copies compared with such copies, copies made from or compared with the original; counterparts of documents as against the parties who did not execute them and oral accounts of the contents of a document given by some person who has himself seen it.[70]

In Evidence Act, 1967, the terms "primary" and "original "are used interchangeably so they are also termed as "copy" and "secondary" evidence respectively of which are akin to the same concept of original and copy, and the secondary evidence must be tendered being compared with the primary one, albeit the secondary one may be admissible on certain circumstances set by the law among them is when the original cannot be obtained. For instance, the court in the case of **Lazarus,**[71] once insisted that an electronic document must comply with the best evidence rule, whenever a party wishes to produce a document in court as evidence, he must provide an original of that document which is called primary evidence.

---

[68] D. R. Mathews, Electronic Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search and Retrieval, Taylor and Francis Group, New York, 2013, 17.
[69] Section 64 of TEA
[70] Section 65 of TEA
[71] Lazarius Mrisho Mafie & Another v Odilo Gasper, Commercial case No.10 of 2008 (Unreported)

2.4 The History and Origin of Electronic Evidence: Worldwide

It is of vital importance, in this chapter to examine the history of documentary evidence to set the background so that in the proceeding chapters be able to determine whether these rules can still be applied today to electronic evidence. The history and origin of documentary evidence is long and convoluted.[72] The history in other words marks the journey from paper era to digital era. The law surrounding documentary evidence has been developed over centuries and has evolved around paper documents.[73] By contrast, electronic evidence has only been in standard use for around 20 years, however, these centuries-old laws are still being applied to electronic evidence.[74] The use of documents in early times appeared as a means to record transfers of land.[75]

During the Norman's feudal system, a charter replaced the ceremony of presenting a twig to the grantee of land .However, general distrust of writing meant witnesses were called, regardless of any inconsistencies. Documents bearing the King's seal became indisputable and this led to common seals being used, which then became a method of authentication. Early cases involving deeds saw the witnesses to the deed, as early as 1208 to 1489 on the jury.[76] This led to 'Trial by Charters' where there could be no claim without a charter, and attesting witnesses had to be called to prove its authenticity.

---

[72] Stanfield (n.39),2
[73] Ibid,2
[74] ibid
[75] ibid
[76] Stanfield (n.39), p.3

It is narrated that the court could not go beyond the Charter and this gave rise to the origin of estoppel by deed and the parole evidence rule.[77] Oral evidence had no place in trial by charter.[78] The doctrines of estoppel by deed developed were solemn and unambiguous statements in deeds were taken as binding. [79]The parole evidence rule emerged to prevent oral evidence being admitted to vary a deed.[80] The history further accounts that soon after, the Statute of Frauds was enacted in England during the 17th Century, which allowed documents to be authenticated if signed by the parties, rather than affixing a seal.[81] Certain contracts were covered, including contracts for the transfer of interest in land, and even today, this requirement still exists, albeit in a more modern form.

Prior to the introduction of machines which could reproduce documents exactly, the best evidence rule applied, which meant that the party wishing to rely upon the document had to produce it or account for its absence. However, a document could not, on its face, prove itself. Several exceptions to the Hearsay Rule for documentary evidence developed over time, most notably the Business Records Exception.[82] This Rule provides that as long as the document was produced in the ordinary course of business, the person who authored the document did not need to attest that the document is what it purports to be, but rather a person who has personal knowledge of the facts can testify about the records.

---

[77] ibid
[78] ibid
[79] https://www.grin.com/document/1021307 accessed on 24/09/2022 at 16;18
[80] Stanfield (n.39),3
[81] ibid
[82] (n.39),3-4

By the end of the 1990s, the World Wide Web (www) offered useable bandwidth and the internet became a functional tool of the workplace,[83] hence the collection of electronic evidence in most countries of the world was inevitable. Moreover, the birth of digital evidence is the result of Federal Crime Laboratory Directors in Washington DC who formed the group known as the Scientific Working Group Digital Evidence (SWGDE) in order to find latent evidence on computer.[84] The concept of electronic evidence was proposed to Federal Laboratory Directors on March 2, 1998 and for the first time in 2002 the Scientific Working Group Digital Evidence published the first book about digital forensics called "Bests Practices for Computer Forensics"[85] Today and having technological development in place, Legislative provisions in various statutes have codified electronic laws on electronic evidence to keep abreast the technological changes and even allow these common law rules that developed over time to accommodate the electronic environment.[86]

2.5 Types of Evidence and differences between Traditional (paper) Evidence and Electronic Evidence

In the advent of technology, the term evidence can now be conveniently categorised into two; the first is traditional/documentary or paper-based evidence and the second is digital or electronic evidence. However, as already hinted in the previous chapter, for purposes of admission electronic evidence, whether is in digital form or as a printout by mechanical means or stored in any electronic device, electronic evidence is the document in Tanzanian laws. Furthermore, unlike traditional evidence, the

[83] https://www.grin.com/document/1021307 accessed on 24/09/2022 at 16;18
[84] Carrie Morgan Whitcomb, 'An Historical Perspective of Digital Evidence: A Forensic Scientist's View' Spring, 2002], Volume 1, Issue 1, International Journal of Digital Evidence, 4
[85] Ibid
[86] Stanfield (n.39),3

terms of real and physical evidence do not technically make sense in the aspect of electronic evidence. In the preceding chapters, it will be extensively discussed how electronic evidence may be regarded as hearsay evidence or direct.

The main difference between paper evidence and electronic evidence is that the latter is digital.[87] Many forms of digital evidence are created on a computer system. The main components of a computer system include hardware and software.[88] Hardware includes the physical components such as the hard disk drive, the keyboard and mouse, the display system and so on.[89] The computer also contains a processor, or central processing unit which contains a number of electrical circuits on silicon chips.[90] Further, the computer will contain a storage device, onto which binary data is written and stored, with storage governed by random access memory (RAM), or similar.[91] The Sedona Conference[92] suggests that the main differences between paper and electronic documents can be broadly grouped into six categories: *(a) metadata, (b) volume and duplicability, (c) persistence, (d) dynamic, changeable content, (e) environment dependence and obsolescence and (f) dispersion and searchability*

2.5.1 Metadata

Metadata is a key feature that differentiates electronic documents from paper documents.[93] In email, metadata will capture essential date records such as Date Sent, Date Received, Date Replied To, Date Forwarded, as well as other metadata

[87] Gultan. (n.15),7
[88] Stanfield (n.39),61
[89] ibid
[90] ibid
[91] Stanfield (n.39),62
[92] ibid
[93] Stanfield (n.39),62

such as To, From, CC, BCC, Sender, Subject and so on. [94] Documents generated by specific applications, such as Microsoft Office, also contain their own metadata.[95] In **Armstrong v Executive Office of the Presiden**t,[96] the United States Court of Appeals, District of Columbia, held that electronic records were records of the federal government and needed to be preserved as such. The court examined the differences between paper records and electronic records, and concluded that the electronic record, particularly email, contained important information, such as who sent and received the document, that was not present in the paper copy. The court said that 'without the missing information, the paper print-outs - akin to traditional memoranda with the "to" and "from" cut off and even the "received" stamp pruned away - are dismembered documents indeed.

2.5.2 Volume and Duplicability

The Sedona Conference not only referred to the volume of electronic information, but called it ‘the rise of crushing volumes of information in the digital realm. Often, the volume of electronic documents, in comparison to hard copy documents, is much greater.[97] Indeed, as the cost of electronic storage devices continues to decrease, it has become much easier for organisations and individuals alike to simply store everything instead of adhering to confusing and time-consuming document deletion policies.[98] The fact that electronic documents are stored in many different locations also adds to the fact that it may be difficult to destroy all copies of documents. Email is perhaps the best example of how electronic documents are quickly created

[94] Ibid,64
[95] Stanfield (n.39), 64 see also https://www2.seas.gwu.edu/~shmuel/WORK/Differences/Chapter%203%20-%20Sources.pdf retrieved on 25/09/2022 at 11:27
[96] 1 F.3d 1274 (D.C. Circuit Court of Appeals 1993 cited in Stanfield (n.112),63
[97] Stanfield (n.39),65
[98] ibid

and replicated. An email will often be sent to more than one recipient, who in turn may forward on the email. The email software used to create and transmit the email automatically creates a copy of the emails as they are sent and resent.

2.5.3 Persistence

Electronic documents are more difficult to dispose-off than paper documents.[99] This is so obvious because a paper can be destroyed by shredding or burning, whereas it is much more difficult to destroy electronic documents, as it is not simply a question of deleting the data on the computer's hard drive. Whenever a file is stored on a computer system, the computer keeps an index of the location of the files on the file storage system such that, when a user retrieves the file, the computer looks up the location of the file in the index, and knows from which sector on the hard drive from which to obtain the file.[100] When a user 'deletes' the file, the computer system removes the file reference from the index but it means that the data for that file still resides on the hard drive part of the computer system, and the space that the file occupied is simply now available to be overwritten by other data. Therefore, 'deleted' data is still able to be retrieved by a computer forensics expert.[101] Therefore, electronic data may be recoverable after a long time it was thought deleted.

2.5.4 Dynamic, Changeable Content

Electronic documents are dynamic and can be manipulated. Further, electronic documents, unlike hard copy documents, are rarely in a fixed final form.[102] It is on this reason that electronic documents are dynamic and changeable, that evidentiary

[99] https://www2.seas.gwu.edu/~shmuel/WORK/Differences/Chapter%203%20-%20Sources.pdf retrieved on 25/09/2022 at 11:27
[100] ibid
[101] ibid
[102] Stanfield (n.39),65

procedures need to examine the computer system in which a document was created and ultimately stored, in order to be sure that the document has not been manipulated in undetectable ways. That is what is known as authenticity test.

2.5.5 Environment-Dependence and Obsolescence

When removed from its environment, electronic data, unlike paper, may be unreadable.[103] Without the proper software application needed to view the data, it would be incomprehensible.[104] For instance, data in a database will be meaningless if the data is removed from the database system in which it was created.

2.5.6 Dispersion and Searchability

Traditionally, hard copy documents were often organised in filing cabinets, with each project having its own file.[105] By comparison, electronic documents typically remain disorganised in disparate locations.

2.5.7 Accessible/Inaccessible

Generally, information, whether it is hard copy or electronic information, may be inaccessible. In **Zubulake v UBS Warburg LLC** (Zubulake 1)[106] Shira Scheindlin J made this distinction between hard copy and electronic documents. Examples of inaccessible paper documents could include: (a) documents in storage in a difficult to reach place; (b) documents converted to microfiche and not easily readable; or (c) documents kept haphazardly, with no indexing system, in quantities that make page-by-page searches impracticable. A further and different example is that documents

[103] Stanfield (n.39),65
[104] ibid
[105] ibid
[106] 217 F.R.D. 309 (S.N.D.Y, 2003).

might be already lost or destroyed.[107]

2.6 General Characteristics of Electronic Evidence

Essentially, electronic evidence is comprised of three main elements, the first being binary data, the second being a storage device on which to store that binary data and thirdly, software to read and interpret the binary data.[108] Due to that nature, it is therefore invisible, easily to be altered or destroyed, involves safety measures to prevent alteration and requires expert demonstration. Although electronic evidence has only been used, in a standard commercial sense, for around 20 years, the forms of electronic evidence are constantly changing.[109]

Social media and cloud computing technologies, such as WhatsApp's, Instagram's, TikTok, Facebook and so many others were not common 20 years ago, and are gaining such widespread acceptance that they will be standard in 20 years' time. As we go on in this current era of rapid growth and development of science and technological revolution may even be superseded by other new forms of technology.

2.7 Conclusion

This chapter tried to discuss relevant aspects to the concept of electronic evidence. The origin of electronic evidence from time immemorial was also traced. The characteristics, and rules applied in admissibility of electronic evidence due to the ephemeral nature of electronic evidence were exposed. The chapter further briefly explained the types of evidence in the two categories of electronic and traditional

[107] Stanfield (n.39),66
[108] Ibid,
[109] ibid p.,65

evidence. Furthermore, differences between traditional evidence and electronic evidence were explained and revealed that they are legally treated differently.

It was revealed from this chapter that the electronic evidence is quite different from traditional or paper-based evidence and hence it needs some peculiar attention during discovery and collection, preservation and presentation to courts for admissibility. It was further learnt that unlike paper-based evidence in all steps where the collection and generation of electronic evidence is at issue, it requires knowledge, expertise and sometimes forensic expertise and collection should be in appropriate and in a secured manner and submitted to courts using reliable services. It was further revealed that procedure for secure seizure and collection of electronic evidence should be established by use of forensic expert to clear out its authenticity so as to prevent higher risk of potential destruction or loss of electronic evidence compared to non-electronic evidence.

Similarly, the chapter disclosed that unlike traditional evidence, electronic evidence is the best evidence in this technological era. For instances, email contains useful and basic information such as “metadata” which aids to capture essential date records such as on what date the email was sent and received, and replied and who sent it and from which computer and from which location, the elements which are not present in paper-based evidence as it was revealed in the case of **Armstrong v Executive Office of the President** (supra).

This chapter generally dealt with an overview on what the electronic evidence, theoretically is all about to have a ground work which paves way to the preceding

chapters. It has some extent attained the goal as it generally disclosed that at the global level the old laws are still applicable to the digital evidence today and therefore diminishing the scope of admissibility of electronic evidence. Chapter three will therefore discuss the law on admissibility of electronic evidence in the Tanzanian jurisdiction.

CHAPTER THREE

LEGAL FRAMEWORK ON ADMISSIBILITY OF ELECTRONIC EVIDENCE IN TANZANIA

3.1 Introduction

This chapter presents the legal framework of admissibility of electronic evidence in Tanzania. The chapter starts by explaining the Constitution of the United Republic of Tanzania being the mother law which the law on admissibility of electronic evidence like any other laws of the land ought to adhere to. The chapter further reviews the relevant electronic laws in Tanzania to see if they have existing provisions suitable to the current technological realities as far as admissibility of electronic evidence is concerned. Finally, is the conclusion showing the insights exposed by the chapter.

3.2 The Constitution of the United Republic of Tanzania, 1977

The laws governing admissibility of electronic evidence aims at dispensation of justice timely and fairly in the administration of justice between the parties. However, dispensation of justice is a constitutional right, which is to be inferred judicially. Therefore, dispensation of justice in the United Republic of Tanzania is the duty of courts as provided for by the Constitution.[110]The said constitution provides that the judiciary shall be authority with final decision in dispensation of justice in the United Republic of Tanzania. Therefore, in order to achieve justice, the laws on procedure of admissibility of electronic evidence must adhere to the constitution. Therefore, the principles of fairness, impartiality, timely, reasonability and accessible for all which are aimed to do justice in the society are constitutional

[110] Article 107A.-(1) of the Constitutional of the United Republic of Tanznaia,1977 as amended from time to time.

tenets which ought to be adhered[111], short of that the judgments pronounced by the courts will be rendered null and void**.** The introduction of the provisions of section 40A,76 and 78A in the Evidence Act vide the Written Laws (Miscellaneous Amendments) Act,2007 and by the enactment of Electronic Transanction Act of 2015 have widely assisted and enabled the courts to discharge properly their constitutional mandate of dispensation of justice for both criminal and Civil cases to parties and the society at large.

3.3 The Evidence Act

Admissibility of Electronic evidence in Tanzania for both Civil and Criminal matters is governed by the Tanzania Evidence Act,[112] the said law is complimented by the Electronic Transactions Act.[113] Most of the rules embodied in TEA trace its origin under common law rules of evidence which applied to traditional evidences in paper-based evidence such as relevance, admissibility, authentication, hearsay, the best evidence and corroboration. TEA received some amendments through the Written Laws, Miscellaneous Amendment Act[114] to accommodate admissibility of electronic evidence in digital environment. Electronic evidence is also admissible in any criminal proceedings.[115]

Section 40A of TEA deals with admissibility of electronic evidence in criminal proceedings while Sections 76,78A are closely related dealing with admissibility of electronic evidence in civil matters but only in banker's books. With the above enacted local electronic statutes,

[111] The Constitution of the United Republic of Tanzania, article 107A(2)(a)-(e); The court should observe the principles of promoting and enhancing dispute resolution among persons involved in the disputes, impartiality, reasonability, not to delay cases and not to be tied by undue technicalities.

[112] The Evidence Act,1967 (TEA) Cap 6 (Now R. E 2019); see in its application section 2; the law applies to judicial proceedings in all courts save the Primary Courts.

[113] Act No.13 of 2015(now R.E 2022); in its long tittle it deals with recognition of electronic transactions-government services, the use of information and communication Technologies in collection of evidence, admissibility of electronic evidence, use of electronic signature and other related matters

[114] The Written Laws (Miscellaneous Amendments) Act,2007 which introduced Section 40A,76 and 78A.

[115] TEA, s 64A (1)

today for both Civil transactions and Criminal activities captured through the use of Technology, retrieved as electronic evidences from digital devices, are admitted in Tanzanian courts of law. Tanzanian law defines electronic evidence to mean "any data or information stored in electronic form or electronic media or retrieved from a computer system, which can be presented as evidence" Alternatively, electronic evidence is any probative information stored or transmitted in digital form; such information can be stored in computer hard drive, optical disks, floppy disks, remote internet storage, handheld devices, memory cards, network servers, emails etc.

Therefore, on account of the above legal definition, just like traditional evidence, electronic evidence is admissible in Tanzanian courts. The court may as well admit data message which is defined as data generated, communicated, received or stored by electronic, magnetic optical or other means in computer syste]m or transmission from one computer to another. The law on Evidence Act has not set a category or explained qualities of witnesses required to tender electronic evidence. This implies every witness or party who wish to prove that some facts exist is competent witness to tender electronic evidence just as it is in traditional evidence. As to issues on emerging practices on tendering admissibility of electronic evidence are discussed in herein below on rules of admissibility of electronic evidence in TEA and ETA.

3.3.1 The Provisions on "*Relevance of evidence rule*"

In Tanzania, for any evidence to be admissible in courts of law it must be relevant evidence. [116] There is close relationship between relevancy and admissibility as for the evidence to be admissible must be relevant to the fact in issue but not all relevant facts are admissible. An

[116] TEA, s.7

admission is a statement, oral, electronic or documentary, which suggests any inference as to a fact in issue or relevant fact and which is made by any of the persons and in the circumstances hereinafter mentioned. [117]

The Evidence Act has provisions which explain how a fact is said to be relevant in admissibility of evidence. It provides that factual evidence which, though not in issue, are so connected with a fact in issue as to form part of the same transaction, are relevant whether they occurred at the same time and place or at different times and places.[118] Facts which are the occasion, cause or effect, immediate or otherwise, of relevant facts or facts in issue or which or constitute the state of things under which they happened, or which afforded an opportunity for their occurrence or transactions, are relevant.[119] Any fact is relevant which shows or constitutes a motive or preparation for any fact in issue or relevant fact.[120]

The conduct of any party, or of conduct any agent of any party, to any suit or proceeding, in reference to such suit or proceeding or in reference to any fact in issue or relevant thereto in the conduct of any person an offence against whom is the subject of any proceeding, is relevant, if such conduct influences or is influenced by any fact in issue or relevant fact, and whether it was previous or subsequent thereto. [121] It is worth noting that to determine that the fact is relevant is a process involving both the party who tenders the evidence and the court. The party tendering electronic evidence must ensure that the evidence is relevant. However, relevant and admissibility of electronic evidence is not straight forward and the law does not expressly prescribe how relevant the electronic evidence may be determined under TEA.

---

[117] TEA, s.19
[118] TEA, s.8
[119] TEA, s.9
[120] TEA, s.10(1)
[121] TEA, s.10(2)

3.3.2 The Provisions on "*Best Evidence Rule*"

The general rule is that all facts, except the contents of documents, may be proved by oral evidence[122] and oral evidence must, in all cases whatever, be direct that is to say it must come from the mouth of the one who perceived it.[123] However, the contents of documents may be proved either by primary or secondary evidence.[124] Primary evidence is the document itself produced for the inspection of the court[125] whereas secondary evidence includes certified copies in accordance with the provisions of the Evidence Act, copies made from the original by mechanical process which in themselves ensure the accuracy of the copy and copies compared with such copies, copies made from or compared with the original, counterparts of documents as against the parties who did not execute them, oral accounts of the contents of a document given by some person who has himself seen it. [126]

The law provides that in order to prove the documents, the primary evidence is the best evidence under the best evidence rule[127] saves to some exceptions where the secondary evidence may prove the documents including where the original has been destroyed or lost or if it is on the custody of the opposite party and the one tendering has given a notice to produce it in court.[128] This originality legacy is derived from a long conventional wisdom that originals are more reliable than duplicates. [129]Alterations or other modifications are more difficult in original material since it is the most convincing evidence available.[130] However, the law by

[122] TEA, s.61
[123] TEA, s.62
[124] TEA, s.63
[125] TEA, s.64
[126] TEA, s.65
[127] TEA, s.66
[128] TEA, s.67 and 68
[129] C. Nemeth, Law and Evidence: A primer for Criminal Justice, Criminology, Law and Legal Studies, Learning, London,2012,141
[130] Ibid

recognising admissibility of electronic evidence in all legal proceedings,[131] the applicability of originality rule under the best evidence rule remains questionable. The provisions of TEA has not explained how the best evidence rule applies in admissibility of electronic evidence neither does it define the original and a copy of electronic evidence.

3.3.3 The Provisions on Hearsay Rule

In criminal proceedings, electronic evidence may be admitted as hearsay evidence as the law says that direct oral evidence of a relevant fact would be admissible, any statement contained in any writing, record or document, whether in the form of any entry in a book or in any other form and which tends to establish that fact shall, on production of the writing, record or document, be admissible as evidence of that fact if the statement was made as a memorandum or record of the act, transaction, occurrence or event; or [132] the writing, record or document is, or forms part of, a record relating to any trade or business and was made or compiled in the regular course of business where it is the practice to record such act, transaction, occurrence or event when it takes place or within a reasonable time thereafter. [133]

All other circumstances of the making of the statement, including lack of personal knowledge by the person making it, may be held as affecting its weight as evidence but those circumstances shall not affect its admissibility.[134] In estimating the weight, if any, to be attached to a statement admissible as evidence by virtue of this section regard shall be had to all circumstances from which any inference can be reasonably drawn as to the accuracy or otherwise of the statement and, in particular, to the question whether or not the person making the statement, or concerned with making or keeping the writing, record or document,

[131] TEA, s.64A
[132] TEA, s.34(1)(a)
[133] TEA, S.34(1)(b)
[134] TEA, s.34(2)

containing the statement, had any incentive to conceal or misrepresent the facts.[135] The term "business" is interpreted to include a business, occupation, profession, trade or calling of every kind and statement" includes any representation of fact, whether made in words or in any other way.

The above provision only mentions admissibility of a document but does not mention electronic evidence. However, the term document is defined to mean any writing, handwriting, typewriting, printing, Photostat, photography, computer data and every recording upon any tangible thing, any form of communication or representation including in electronic form, by letters, figures, marks or symbols or more than one of these means, which may be used for the purpose of recording any matter provided that recording is reasonably permanent and readable.[136]

The Tanzanian provisions generally treat electronic evidence as hearsay evidence without describing whether it is computer stored or computer generated.[137] Electronic evidence is thus admitted under hearsay exceptions rule as the law further provides that any criminal proceedings where direct oral evidence of a relevant fact would be admissible, a written or electronic statement by any person who is, or may be, a witness shall subject to the following provisions of this section, be admissible in evidence as proof of the relevant fact contained in it in lieu of direct oral evidence.[138]

The law provides further that a written or electronic statement may only be admissible under this section where its maker is not called as a witness, if he is dead or unfit by reason of bodily

[135] TEA, s.349(3)
[136] TEA, s.3(1)(d)
[137] Crossey,N.E(n.47),p.560
[138] TEA,s.34B(1)

or mental condition to attend as a witness, or if he is outside Tanzania and it is not reasonably practicable to call him as a witness, or if all reasonable steps have been taken to procure his attendance but he cannot be found or he cannot attend because he is not identifiable or by operation of any law he cannot attend or if the statement is, or purports to be, signed by the person who made it including so many circumstances.[139] The hearsay rule has no link to other rules like reliability, integrity and authentication rule. For instance, scholars argue that it is not justifiable by the court regarding the evidence as hearsay through interpretation of direct or original evidence rule and refuse to admit them.[140]

In electronic evidence, so long as there is no issue as to whether computer was functioning properly or otherwise there was no misuse the electronic evidence is not subject to hearsay.[141]Under TEA, because every witness is competent to tender electronic evidence provided should prove to court with accompanying affidavit that the computer was functioning properly[142]. The said provision talks only on bankers' book and the person to swear affidavit is an officer in charge of the computer. The inadequacy of the law involving no digital profession for evidence retrieved from digital devices like emails would cause rendering electronic evidence hearsay.

The provisions on TEA which apply for admission of electronic evidence in criminal proceedings under the hearsay exceptional rule are less or more similar to civil proceedings. The law provides that in any civil proceedings where direct oral evidence of a fact would be admissible, any statement made by a person in a document tending to establish that fact shall,

[139] See sections34B(1)(a) and 34B(2)(a)
[140] Mohamed. A, admissibility of electronic evidence in the court of Malaysia and United Kingdom, International journal of law government and communication, Vol 4,Iss.No.15,2019,p.126 retrieved from http://www.eij lgc.com at 17:21 on 10/10/2023
[141] Stanfield n.39, p.203
[142] Section 78(2) of TEA.

in production of the original document, be admissible as evidence of that fact in lieu of the attendance of the witness if the following conditions are satisfied.[143] It is argued that digital versions of statements are therefore documents admissible to the same extent as paper -based statements, provided the requirements of form and signature are complied with.[144]

Banker's books may also be admitted as electronic evidence.[145] A copy of an entry in a banker's book shall not be received in evidence under this Act unless it is first proved that the book was at the time of the making of the entry one of the ordinary books of the bank and that the entry was made in the usual and ordinary course of business, and that the book is in the custody or control of the bank.[146] Such proof may be given by an affidavit sworn before any commissioner for oaths or a person authorised to take affidavits.[147]

A print out of any entry in the books of a bank from a computer or any electronic device obtained by a mechanical or other process which in itself ensures the accuracy of such print out, and when such print out is supported by a proof of affidavit that it was made in the usual and ordinary course of business, and that the book is in the custody of the bank, it shall be received in evidence under TEA.[148] Any entry in any banker's book shall be deemed to be primary evidence of such entry and any such banker's book shall be deemed to be a "document" for the purpose of admission as electronic evidence.[149]

A copy of any entry in a banker's book shall not be received in evidence unless it be further proved that the copy has been examined with the original entry and found to

[143] TEA, s.34C(1)
[144] Stanfield n.39, p.206
[145] TEA, s.76
[146] TEA, s.78(1)
[147] TEA, s.78(2)
[148] TEA, s.78(1)
[149] TEA, s.78(2)

be correct.[150] Furthermore, such proof shall be given by person who has examined the copy with the original entry, and may be given either orally or by an affidavit sworn before any commissioner for oaths or a person authorised to take affidavits.[151] TEA also recognises the admissibility of private and public documents.[152]

3.3.4 The Provisions on Corroboration Rule

The law, whether in civil or criminal proceedings does not require collaboration to electronic evidence as it is explicitly provided that for the purposes of any rule of law or practice which requires that evidence be corroborated or regulates the manner in which uncorroborated evidence is to be treated, a statement admissible under this section shall not be treated as corroboration of evidence given by the maker of the statement.[153] However, Thomson argues that corroboration is an essential tool for the successful presentation of electronic evidence as it can be done through a combination of witness testimony and documentary and physical evidence that address particular points in the case, and take into account the content and context of the evidence. For example, consistent testimony by unrelated witnesses about a particular event can indicate reliability. [154]It is not legislated under TEA how electronic evidence can be collaborated with other electronic evidence or accompanying evidences.

3.3.5 The provisions on Authentication Rule

The law which governs authenticity of electronic evidence during admissibility of electronic evidence is the Electronic and Transactions Act (ETA) as is provided in TEA that the admissibility and weight of electronic evidence shall be determined in the manner prescribed

[150] TEA, s.79
[151] TEA, s.39
[152] TEA, s.82 and 84
[153] TEA, s.34B(6) and 34C (7)
[154] Thomson (n.33), p.5

under section 18 of the Electronic Transaction Act. Now the in following section is the analysis of the rules of admissibility and authentication under ETA.

3.4 The Electronic Transactions Act

The law which governs authenticity of electronic evidence is the Electronic and Transactions Act (ETA) as is provided in TEA that the admissibility and weight of electronic evidence shall be determined in the manner prescribed under section 18 of the Electronic Transaction Act[155]. ETA takes a lead and supersedes other laws on matters of admissibility of electronic evidence as it provides that there should be no any rule of evidence in any legal proceedings which shall apply to deny admissibility because it is a data message.[156] As said earlier, in its long tittle, ETA was an Act to provide for legal recognition of electronic transactions, e-Government services, the use of Information and communication Technologies in collecting evidences, admissibility of electronic evidence, to provide for the use of secure electronic signature; and provide for other related matter.[157]

The Act provides criteria for determining reliability, admissibility, authenticity and assessing weight of data message. [158] In determining admissibility and evidential weight of a data message, the following shall be considered (a) Reliability of manner in which the data message was generated, stored or communicated (b) Reliability of the manner in which integrity of data message was maintained (c) The manner in which the originator was identified; and (d)any other factor that may be relevant in assessing the weight of evidence.[159] Section 18(3) further talks on the conditions in which authenticity of electronic record system

[155] TEA, s.40A(2)
[156] ETA, s.18(1)
[157] ETA on its long tittle.
[158] ETA, s.18
[159] ETA, s.18(2)

is presumed in favour of admissibility of electronic business records. This is the presumption of regularity and it implies that when the admissibility of electronic evidence under section 18(1) of ETA is at issue, section 18(3) of conditions for authenticity automatically comes into play.

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 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,[160] (b) it is established that the electronic record was recorded or stored by a part to the proceedings who is adverse in interest to the part seeking to introduce it; [161] or (c) it is established that an electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a part to the proceedings and who did not record or store it under the control of the part seeking to introduce the record[162] (4) 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.[163]

The law extends that where a written law requires a person to produce a document or information, that requirement is met if- (a) the person produces, by means of an electronic

[160] ETA, s.18(3)(a)
[161] ETA, s.18(3)(b)
[162] ETA, s.18(3)(c)
[163] ETA, s.18(4)

communication, an electronic form of that document or information; (b) considering all the relevant circumstances, at the time that an electronic communication was sent, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of integrity of the information contained in the document; and (c) at the time that an electronic communication is sent, it is reasonable to expect that an information contained in the document or information would be readily accessible so as to be usable for subsequent reference.[164] For the purposes of this law the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for the addition of any endorsement; or any immaterial change, which arises in the normal course of communication, storage or display.[165]

3.5 The Cybercrimes Act

The Cyber Crimes Act of 2015, being a penal law, which creates offences committed through the aid of computer also, has some provisions touching on electronic evidence in criminal matters particularly in investigation, collection and use of electronic evidence. Therefore, currently courts just like in civil wrongs proceedings are at liberty to receive and admit electronic evidence in cybercrimes. The Cyber Crimes Act provides on the law of search, seizure and collection, preservation of electronic evidence in relation to admissibility.

As far as search and seizure of electronic evidence issues are concerned, the law provides that the police officer in charge of a police station or a law enforcement officer of a similar rank, upon being satisfied that there are reasonable grounds to suspect or believe that a computer system may be used as evidence in proving an offence or is acquired by any person as a result

[164] ETA, s.20(1)(a), (b) and (c)
[165] ETA, s.20(2)

of an offence, may issue an order authorizing a law enforcement officer to enter into any premise and search or seize a device or computer system and secure the computer data accessed or search any other computer which the data is stored in accordance with the law regulating search and seizure. [166]

Apart from power to search, the police officer in charge of a police station or a law enforcement officer has also where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, a power to issue an order to any person in possession of such data compelling him to disclose such data.[167] In case the exercise is not possible the police officer will apply for the court order to compel that person to disclose such data.[168]

Concerning collection of electronic evidence, the enforcement officer during investigation and prosecution may issue and order for disclosure, collection or recording of the traffic data associated with a specified communication during a specified period or permitting and assisting the law enforcement officer to collect or record that data.[169] For the purposes of this section, "traffic data" means- (a) information relating to communication by means of a computer system; (b) the information generated by computer system that is part of the chain of communication; and (c) information that shows the communication's origin, destination, route, time, size and duration. Technical means such forensic tools from forensic expert may be deployed.[170] As far as preservation is concerned an order may be issued requiring the person in control of a device or computer data to preserve the device or computer data for a

[166] CCA, s.31(1) and (2)
[167] The Cybercrimes Act, s.32
[168] CCA, s.32(3)
[169] CCA, s.34(1)
[170] CCA, s.34(2)

period not exceeding fourteen days.[171] However, the court may, on application, extend such order for such period as the court may deem necessary.[172]

TEA and ETA have no explicit provisions guiding collection, preservation and presentation of electronic evidence. There are neither provision which governs the role and duty of computer forensic expertise or any person to collect, preserve and retrieve electronic evidence up to the stage of admissibility of electronic evidence in courts save The Cyber Crimes Act which has the said provisions governing on collection, seizure of electronic evidence but they only regulate electronic evidence on criminal matters only as the said law does not apply in civil matters.

3.6 Conclusion

This chapter dealt with the legal framework of admissibility of electronic evidence in Tanzania by first analysing a Tanzanian constitution which is the base of justice upon relevant laws of admissibility of electronic evidence ought to adhere. It was shown that, if the court, during admissibility of electronic evidence, does not adhere to the constitution, its end result judgments will be declared void and null. It was found that the introduction of electronic evidence has assisted the courts to dispense their constitutional mandate in dispensation of justice fairly between parties. The Evidence Act was reviewed and found that it provides the codified common law rules of admissibility notably hearsay, collaboration, authentication, relevancy and best evidence rules. It was further found that neither the Evidence Act nor the Electronic Transactions Act has provisions regulating on collection, seizure, search

[171] CCA, s.35
[172] CCA, s.33(2)

and preservation save the Cybercrimes Act. However, they only regulate in criminal matters since the said law is the penal one.

It was disclosed that Tanzania Evidence Act has been amended to respond changes brought by technological development and new digital laws have been enacted by bringing new digital provisions which govern admissibility of electronic evidence. Nonetheless, Evidence Act still contain common law rules applied in paper-based evidence of which still apply in equal or less similar with electronic evidence. The chapter learnt that the Electronic Transactions Act came with the provisions on authentication, reliability and integrity of electronic evidence but yet they are insufficient and not comprehensive as a result courts do interpret them inconsistently and heterogeneously.

Moreover, the Cyber Crimes Act have some provisions governing rules on collection, seizure of electronic evidence but they deal with such aspect only in criminal matters and not civil matters. Moreover, the Cybercrime provisions on collection and seizure as they appear do not observe a constitution and privacy rights during search, collection and seizure of electronic devices carrying electronic evidence. Again, the rules on admissibility of Electronic Evidence in Tanzania are scattered which becomes hard for courts to interpret and hence inconsistent application and cause injustices in the society since admissible evidence are disregarded and vice versa.

The study revealed that it is not clear whether the electronic document or evidence is the Primary evidence or secondary evidence. The TEA which is the principal Act

still talks that the certified copies from the original by mechanical process are secondary evidence but does not define what is the secondary of electronic evidence the fact which may bring confusion to courts during admissibility of electronic evidence and a cause of unpredictable decisions in the same court. Some provisions are lagging behind as in electronic evidence originality rule cannot be applied just like in paper-based evidence.

The study further disclosed that electronic evidence in Tanzania is generally treated as Hearsay evidence without the law categorising whether the evidence is computer generated or computer stored evidence. It has been disclosed in previous chapters that computer generated is not hearsay save computer stored evidence. The chapter yielded that The Electronic Transactions Act is the specific law determining reliability, admissibility, authenticity and assessing weight of data message and section 18 of the same law prohibits any rule of evidence to be used to deny admissibility of electronic evidence in any legal proceedings which is the confusion as TEA contains the rules on admissibility of electronic evidence and is the principal Act. But again, this implies that the rules in ETA are more inclusionary than exclusionary which is likely to allow evidence which ought not be admissible to be admitted and hence causing injustices.

The chapter further observed that ETA of 2015 do not stipulate the comprehensive procedural safeguard of uniform authenticity of electronic evidence for courts to follow from collection, preservation up to the stage of presentation to courts for admissibility. ETA being a law governing authenticity of electronic evidence does not talk anywhere about authentication by use of certificates or affidavits save the

provision of TEA and they only refer to banker's books independent from other types of electronic evidence such as social media which is prevalent to this technological era.

The Cyber Crimes Act though talks about investigation, search, seizure, arrest and collection of electronic evidence but the law only deals with criminal electronic evidence. But also, the law is not exhaustive in the letters of collection and preservation of electronic evidence by observing privacy and person data protection as well as human rights set international. This is possibly up to this time when the research data is collected there is yet no privacy and personal data protection in Tanzania. For instance, the Cybercrimes Act allows any police officer in charge of a police station to issue an order to arrest and seize any electronic device for a suspect of an offence and collect evidence without even a court order.

CHAPTER FOUR

CHALLENGES RELATING TO ADMISSIBILITY OF ELECTRONIC EVIDENCE IN TANZANIA

4.1 Introduction

This chapter mainly provides general challenges of admissibility of electronic evidence in the Tanzanian context. It begins by an overview of discussion on what are the challenges of admissibility of electronic evidence in the advent of technology. The chapter engages views from legal scholars, review from regional instrument like Commonwealth Model Law of ecteronic evidence to explore the challenges. The chapter will show that there are serious efforts and commitment done under national, regional and global level to curb the challenge of admissibility of electronic evidence brought up by the development of technology.

It will be shown that there are electronic rules already put in place such under regional level such as Commonwealth a model law on admissibility of electronic evidence to guide member countries and reduce challenges. Additionally, the chapter highlights the modern procedure on collection of electronic evidence which should balance between security and privacy rights which has direct impact to the required international standard on admissibility of electronic evidence. Thereafter, the chapter provides different jurisdictions of the world that have dealt with the challenges of authentication and admissibility of electronic evidence.

The two countries USA and UK which are developed countries in technology have been set as example on issues of admissibility and authentication of electronic evidence to explore the challenges through reviewing some legislations and tested

case laws. Although Tanzania and USA do not share the same legal system but technology looks no boarders as challenges disclosed in one country can be a lesson to solutions for challenges in another country. Lastly the chapter concludes to indicate the main insights obtained under the chapter.

4.2 Challenges of Admissibility of Electronic Evidence in Tanzania

Review from Tanzanian scholars and practitioners reveal that original physical items should be the subject of one of the exclusionary standards. Starting from this premise, this section explores the challenges caused by the preference for original evidence, and the reasons for the rigorous standard of admissibility for electronic evidence in Tanzania judicial practice. The said challenges include a misunderstanding of the theory of admissibility for electronic evidence, indicating a misunderstanding between admissibility and weight or probative value, regarding every electronic evidence as hearsay and absence of authentication procedure in admissibility of electronic evidence. The challenges are exacerbated by the influence by the evidentiary standard, neglecting the important function of authentication, and the lack of knowledge of electronic evidence. The ephemeral nature of electronic evidence, being known that it is easy to alter or tamper with electronic evidence wrongly goes to the weight rather than the admissibility of the evidence.

Electronic evidence can be authenticated by other circumstance evidence, rather than preventing suspicious evidence from being admitted into legal proceedings. The digital world has become a main source of evidence, and the admissibility and the weight of electronic evidence has become an unavoidable issue for lawyers and judges. However, because electronic evidence is not a physical object, but only

exists as digital data stored on tangible carriers, there is an argument in Tanzania over which kind of electronic evidence is reliable, believable and authentic.

Therefore, the challenges where there is no explanation about compliance to rules over its collection process, and where it is collected through illegal methods are prevalent. The insistence by courts that electronic evidence should be presented without the original physical items is a misunderstanding towards the conception of 'original' in terms of electronic evidence, and without a clear definition of what the original is, valuable electronic evidence would be excluded inevitably. The interpretation of the High Court in Tanzania on the digital rules of admissibility of electronic evidence is inconsistent which itself is also the major challenge as will be explored herein below.

4.2.1 Admitting Electronic Evidence being Influenced by the Preference for Originals: The Best Evidence Rule Challenge.

It has been a long-known rule that to secure the authenticity and credibility of evidence, an exhibit should be original.[173] Many laws in various jurisdictions require electronic evidences to be submitted in original forms just like traditional physical evidence.[174] It is worth making a point clear from the outset that in Tanzania Evidence Act, 1967, the terms "primary" and "original "are used interchangeably just they are on "copy" and "secondary" evidence of which are akin to the same concept of original and copy, and the secondary evidence must be tendered being compared with the primary one, albeit the secondary one may be admissible on

[173] Liu.B.(n.31), p.39
[174] Ibid, P.39

certain circumstances set by the law among them is when the original cannot be obtained.[175] The same concept of original legacy is still playing an important role in our judicial courts during admissibility of electronic evidence. For example, in *Ivanna Felix Teri vs Viettel Tanzania Public Limited Company and another*[176] the High Court among others insisted the production of the original photo to be compared with the tendered copy and therefore among other reasons accorded no weight to the tendered copy of generated photography alleged to have been taken from Instagram and Facebook.

It appears that the said originality legacy in the advent of technology challenges the current digital laws as was revealed in most high court cases which were interpreted immediately after introduction of new digital laws in Tanzania. The high Court, in its numerous decisions said that an electronic document must comply with the best evidence rule whenever a party wishes to produce a document in court as evidence; he must provide an original of that document which is called primary evidence.[177] Besides the court has not clarified how secondary evidence of an electronic document may be produced in legal proceedings nor did the court define original evidence of electronic evidence and therefore remains a big challenge.

In Emmanuel Godfrey Masonga's case (Supra) for example the court observed that data recorded in the cell phone that was lost was the original document. It simply

[175] TEA, s 64,65&66

[176] Civil Case no. 7 of 2019, High Court of Tanzania at Moshi (Unreported)

[177] Fadhili Mbwana vs Raymond William Komba DC Civil Appeal No.06 of 2022, HCT at Songea (Unreported),Lazarius Mrisho Mafie & Another v Odilo Gasper, Commercial case No.10 of 2008 (Unreported), Emmanuel Godfrey Masonga v Edward Franz Mwalongo Misc. Civil cause no.6 of 2015, HCT (Iringa District Registry) Njombe, (Unreported) and William Joseph Mungai v Cosato David Chumi, Misc. Civil Cause No.8 of 2015, HC (Iringa District Registry), Iringa (Unreported.)

said the VCD that was made, could be produced as secondary evidence without further clarification of laying foundation. In that regard, Scholars therefore argue that authenticity of electronic evidence is still bound by its primitiveness, and the concept of original played an important role in deciding authenticity but today the concept of original cannot be applied to electronic evidence in the same manner as paper-based evidence.[178] The challenge extends where legislators and practitioners put much emphasize to original items, it is therefore not hard to conclude that it is a preference for original physical items which acts as admissibility standard in admissibility of electronic evidence.[179]

Going with the trend of requiring electronic evidence to be submitted with the original physical evidence we will be missing a point on the definition of original electronic evidence. This is because it has been observed that telling the difference between the original physical and copy of electronic evidence is a problem itself.[180] In August, 1998, the Scientific Working Group on Digital Evidence defined original digital evidence as physical items but includes all digital data in whatever form.[181] By this definition, it can be grasped that the range of electronic evidence is not limited to those with original physical items but includes all digital data in whatever form. This is interpreted to mean that the significance of producing the original copy of electronic evidence lies in the metadata or a data fingerprint which can be very useful information and importance for authentication of electronic evidence.

[178] Liu.B (n.31), p.39
[179] Ibid
[180] Makulilo A. B, The Admissibility of electronic evidence in Tanzania: new rules and case law, (n.25), p. 121
[181] Liu.B (n.31), p.39

But sincerely the storage medium may be difficult to identify or present at the trial. For instance-mails, web-based instant chat records, web pages, cloud stored information etc. The "original" can only be their digital content at the time of collection which may occur in different formats without altering the original information. This means it is not possible to say which one is the original or how many originals exist.[182] Therefore, the physical item of storage is just part of the original electronic evidence. It is therefore argued that the traditional standard for original and their copies do not apply in the digital world. Holding preference for original in admissibility of electronic evidence results in to the complexity of identifying the original as electronic evidence is different from video or audio in analogue format, which is in form of physical evidence, and can be relatively easily to identify.

Mason after his investigation echoes that the concept of original cannot be found in digital object in whatever form it takes.[183] He suggested that it is necessary to reconsider the conceptual frame work which many lawyers have failed to do. Mason further discovered that the nearest we can get to the concept of an original in digital object is to recognise that it is necessary to consider how authentic the digital object is. The said scholar therefore enumerated three criteria to consider so as to admit electronic evidence just as the original physical could be admitted, as follows*: (a) The content of the data that a party relies upon has not changed from the moment it was created to the moment it was submitted as evidence. (b)The data can be proven to be from the purported source(c)The technical and organisational evidence*

[182] Liu.B (n.31), p.39
[183] Mason, Electronic evidence and the meaning of original, (n.41)

demonstrates the integrity of the data is trustworthy and is therefore considered reliable. Therefore, what we can learn from this scholar is that the court has to lay foundation of electronic evidence as per Mason's above criteria and if satisfied, should ultimately admit electronic evidence under the best evidence rule irrespective of whether it was original or not, which is in fact hard to comprehend due to the nature and characteristics of electronic evidence.

Therefore, many scholars agree that the adoption of the concept of an original physical item as the basis of exclusionary criteria for electronic evidence diminishes the concept of electronic evidence, and eliminates the possibility of producing or admitting electronic evidence with probative value, which now remains as a legal challenge in our courts. Realising that the already enacted rules of evidence are not modernised to quench the thirsty of technological needs, the Commonwealth countries including Tanzania found it necessary to draft the Commonwealth Model Law of electronic evidence[184] as the model law to the member countries so as to mitigate and minimize the challenges of admissibility of electronic evidence.

This Model Law on Electronic Evidence aims to provide such a framework for the admissibility and treatment of electronic records in the context of civil, criminal or administrative proceedings in a court or before a tribunal, board or commission. The Model Law contains provisions on general admissibility, the scope of the model law, authentication, application of best evidence rule, presumption of integrity, standards,

[184] The Commonwealth Model Law on Electronic Evidence,2017 is the work of Commonwealth secretariat. The Model Law draws on the Singapore Evidence Act Section 35 (1), the Canada Uniform Electronic Evidence Act, and the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce.

proof by affidavit, cross examination, agreement on admissibility of electronic records, and admissibility of electronic signature.

The draft model is the work of Law Ministers and Attorney-Generals of Small Commonwealth Jurisdictions, at their 2000 meeting who recognized that common law rules of evidence were not adequate to deal with technological advances and needed to be modernised. They welcomed the convening of an Expert Group to develop model legislation on electronic evidence to address the needs of small Commonwealth jurisdictions. The Expert Group examined the admissibility of electronic evidence and the question whether the rules that apply to other forms of documentary evidence can be applied in a like manner to electronic documents. The outcomes of the work of the Expert Group in the form of the draft Model Law on Electronic Evidence were submitted to Commonwealth Law Ministers at their meeting of 18-21 November 2002, held in Kingstown, St Vincent and the Grenadines.

Law Ministers commended the Model Law for use by those Commonwealth member countries seeking assistance in the development of an appropriate legislative framework. Law Ministers further observed that the Model Law adapts the general rules of evidence to meet new technology possibilities and realities. It is from this common wealth instrument which gave rise to the national law of Tanzania to wit Electronic Transactions Act,2015 as section 18(1) and (2) of ETA are based on article 9(1) and (2) of the UNCITRAL Model law on Electronic Commerce which deal with admissibility and evidential weight of data message respectively.[185]

[185] Setthapirom, W, The Collection of Electronic Evidence in the Prevention of Cybercrimes A Dichotomy Between Security and Privacy, Orebro University,2021, p.15

Member countries wishing to make use of the Model Law on Electronic Evidence may choose to do so as a separate piece of legislation; as part of a law on electronic transactions; as amendments to existing laws on evidence; or as part of a process of modernisation of evidence law that concentrates primarily on criminal law matters and business records in their more traditional sense. The model has the provision which sets the scope of admissibility of electronic evidence. The Model declares that nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record. However, the Act states that the Act does not modify any common law or statutory rule relating to the admissibility or records, except the rules relating to authentication and best evidence. Therefore, the court applying this Act is allowed under this law to have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.

It appears that through this instrument, the primitive originality legacy rule has been neutralised in the advent of technology and is no longer a complex challenge. Since it spells that the person seeking to introduce an electronic record in any legal proceeding to have the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.[186] Similarly, concerning the Application of Best Evidence Rule, spells that in any legal proceeding, subject to subsection (2), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.[187] In any

[186] Commonwealth Model Law on Electron Evidence, Rule 5
[187] Commonwealth Model Law on Electron Evidence, Rule 6. (1)

legal proceeding, where an electronic record in the form of printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purposes of the best evidence rule.[188] This is interpreted to mean that there will be no secondary or original documentary evidence in electronic evidence what is needed is to lay down foundation on the integrity and authenticity of the document to prove that what the document is what the person claims to be.

4.2.2 Absence of necessary Knowledge or Guiding Rules during Collection, Preservation and Admissibility of Electronic Evidence

Electronic Evidence needs knowledge from the time of collection up to tendering stage. It can be difficult to determine its origin, creator and modification after its formation and to identify its authenticity and integrity. The challenges come therefore for developing countries like Tanzania as not every person or institution may have such ability of employing apparatus and equipment due to low level of technology. Conversely, compared to traditional evidence whereby any person may have even a lay knowledge on how to preserve and collect such evidence. In undertaking electronic evidence, computer forensics experts or internet service providers are needed to perform such duties.[189]

The Tanzania law provides for the admissibility or the handling of electronic evidence without involving digital evidence professionals.[190] The absence of such necessary knowledge means there is a risk that Tanzania admits evidence which

[188] Commonwealth Model Law on Electron Evidence, Rule 6.
[189] Ubena.J (n.30),62
[190] Ibid

ought to have not been admitted and vice versa.[191] It is suggested that to preserve and provide digital information should be a legal obligation for internet service providers therefore there should be a regulation providing the content information as well as its publishing time, IP address, domain name and switching information; and Internet Service Providers (ISP) should record and preserve the user's information including the on-line time, account number, IP address or domain name.[192]

In contrast, in USA for instance a role of an expert is recognised as a witness with knowledge testifying that an item is what it is claimed to be[193] again an expert may also state an opinion and give the reasons on electronic evidence without first testifying to the underlying facts or data.[194] However, the expert may be required to disclose those facts or data on cross examination.[195] An expert will tell the court on distinctive characteristics and the like, the appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.[196]

This expertise provides affidavits or testimony about the collection or production process of the information when necessary, and this scenario is so common that major internet service providers have a special department to handle these requests.[197] Because they act as neutral third parties and, digital information provided by them is more credible and requires relatively simpler authentication

[191] Ubena,(n.30),p.62
[192] Michael J. Hannon. Digital Evidence-computer forensics and legal issues arising from computer investigations (William S. Hein & Co., Inc., 2012), at 331.
[193] Federal Rules of Evidence, Rule 901(b) (1)
[194] Federal Rules of Evidence, Rule 705
[195] Federal Rules of Evidence, Rule 705
[196] Federal Rules of Evidence, Rule 901(b) (4)
[197] Liu. B (n.31), p.43

procedures.[198]

It appears that Electronic Transactions Act and Evidence Act have are no clear rules on collection, preservation and presentation of electronic evidence which govern the role and duty of computer forensic expertise before admissibility of electronic evidence in Tanzania. The Cyber Crimes Act have some provisions governing rules on collection, seizure of electronic evidence but they only regulate electronic evidence on criminal matters only as the said law does not apply in civil matters. However, the said provision as they appear does not observe privacy and personal data protection as per international standard.

Any measure which entails the collection, preservation, search and seizure of evidence must be based on a legal basis.[199] The requirement of a legal basis for the adoption of investigative measures is prevalent in all legal frameworks.[200] However, the collection and use of e-evidence has hardly been addressed in Tanzanian evidence laws. However, for instance in Europe, they have guidelines directing that electronic evidence should be stored in a manner that preserves readability, accessibility, integrity, authenticity, reliability and, where applicable, confidentiality and privacy.[201] In Tanzanian laws, rules providing minimum safeguards to data privacy and technical measures are still imprecise and vaguely formulated as the Data protection Act is still in its nascent stage. Legal practitioners in Tanzania must

[198] Liu. B (n.31), p.43
[199] Setthapirom, W, The Collection of Electronic Evidence in the Prevention of Cybercrimes A Dichotomy Between Security and Privacy, Orebro University,2021, p.15
[200] Ibid
[201] Guidelines and Explanatory memorandum on electronic evidence in civil and administrative proceedings adopted by the Committee of Ministers of the Council of Europe on 30 January 2019.

be aware and knowledgeable on all these issues in relation to admissibility of electronic evidence.

Additionally, the process of collecting, storing and processing electronic evidence itself must be understandable to the court. This is a problem to our Tanzania court system as most of the personnel presiding before the court and other officers of the court do not have enough knowledge on the issue of cyberspace hence more effort must be used to convince the courts upon collected evidence.

However, it appears that, lack of knowledge during admissibility cuts across many jurisdictions. For instance, In India it was reported that the lower judiciary in India are largely technologically unreliable, and do not appreciate the authenticity issues or ensure safeguards while allowing the admission of electronic evidence, barring a few exceptions.[202] The decisions of the Supreme Court set up a further precedent for the lower judiciary to appreciate the special procedure prescribed for electronic evidence. Scholars specifically suggest that the best guide rules to judicial officers and lawyers are needed to impart knowledge and guide them while dealing with admissibility of electronic evidence.[203] When a lawyer wishes to establish facts that original evidence can prove, the lawyer should not rely on irrelevant evidence to prove such facts.

The American case of *Perforaciones Martimas Mexicana S. A de C. V v Seacor Holdings*,[204] before Kent J in the United States District Court S.D Texas, Galveston

[202] Anand, A et al, (n.38),35
[203] Ibid
[204] 443 F. Supp. 2d 825, 832 (S.D. Tex. 2006).

Division, explains the issue of lack of knowledge as the plaintiff sought to prove that there was in existing joint venture. They did not produce the relevant documents as proof, but just referred the court to publication from the internet. This was not accepted by the judge, partly because the contract was not provided to the court and it was not appropriate to use information from the internet as proof.

4.2.3 Misunderstanding the Difference between Admissibility and Weight of Evidence

The more relevant information collected, the more precisely the facts can be ascertained, so some information should not be excluded recklessly due to its uncertainties. Physical evidence or paper documents can be forged, and the witnesses' competence can be questioned due to their youth or perceptive defects but all these elements would affect the weight of evidence and not the capability of giving evidence. Similarly, electronic evidence should not be excluded simply because of its vulnerability of being tempered or altered.[205] For instance, in United states Courts have held that the mere possibility of alteration is not sufficient to exclude electronic evidence, in the absence of specific evidence of alteration.[206] Such possibilities go only to weight of evidence not admissibility of evidence.[207]

Weight of evidence goes to the merit of the evidence to be tendered and is normally determined by the court after the evidence has been admitted and valuated in totality to accord it a probative value. However, it appears that the Electronic Transaction Act, 2015 under section 18(2)[208] appears to have conditions for evidential weight but

[205] Liu.B (n.31), p.40
[206] Ibid.p.40
[207] Ibid
[208] ETA, Section 18(2)

not conditions for admissibility and a close look on the entire provision suggests that the law has placed the criteria for admissibility and weight of evidence in the same footing, the factor which may diminish the possibility of admitting electronic evidences.

The entire scheme of Electronic Transactions Act has not been read in by the High Court of Tanzania together Evidence Act as many cases decided on the new ETA depicts the paradox and inconsistences during interpretations. For example, the court in *Emmanuel Godfrey Masonga and William Joseph Mungai*(supra) have erroneously applied the criteria in section 18(2) of ETA to determine admissibility of electronic evidence in section 18(1). Accordingly, in both cases they have all relied on section 18(2). Although the court in William Joseph Mungai did not go further to evaluate how the criteria in this sub section were met but correctly held that the question of weight of the audio CD could be tested through cross examination.

One scholar has observed that the world "admissibility" which inadvertently appears in section 18(2) of ETA might be the source of this confusion.[209] However, on a reflection to ETA only the case of William Joseph Mungai(supra), the court overruled the objection against the production of audio CD on the mere assertion that the audio CD, being in digital form, was easily tampered with. Many cases till to date have followed such criteria. For instance, In *Fadhili Mbwana vs Raymond William Komba,*[210] the High while deliberating on whether the lower court Courts legally admitted electronic evidence in form of print out, brought into play many

[209] Makulilo A. B, The Admissibility of electronic evidence in Tanzania: new rules and case law, Digital Evidence and Electronic Signature Law Review (n.34), p.124

[210] DC Civil Appeal No.06 of 2022, HCT at Songea (Unreported)

provisions under TEA which are applicable to paper-based evidence read them together with section 18 of ETA and thus unnecessarily raised a strict and higher standard and decided that the print out was secondary evidence and that the proof must be by primary document without expounding how the primary electronic evidence could be tendered. The court ended by expunging the same that it ought to have not been admitted.

Just to borrow a leaf, in Germany, for instance electronic evidence is usually regarded as preliminary evidence, and the admissibility and probative value is decided by judges'discrition. Authenticity and integrity are two main factors in evaluating its probative value.[211] Briefly, in America and Germany, the uncertainty of electronic evidence affects the weight and not the admissibility. It is suggested that to adopt high admissibility criteria for electronic evidence and to exclude such evidence due to the insufficiency of authenticity misses the difference between the admissibility and weight of electronic evidence. To show that the confusion between weight and admissibility is the global challenge, the below demonstrated research conducted in China underscores the point. A survey of 69 criminal judges (including assistant judges) from a northern city in China showed that criminal cases, when evaluating electronic evidence, quite a portion of judges do not distinguish between admissibility and weight because of lack of awareness, or for avoiding unnecessary troubles; they determine the admissibility and weight at the same time.

In addition, many judges did not know how to evaluate admissibility and weight. It is not surprising that if similar research was also to be conducted in Tanzania

[211] Liu. B (n.31), p.41

possibly it would have yielded the same result as it is evident from Tanzanian case law. For instance, in *Ivanna Felix Teri vs Viettel Tanzania Public Limited Company and Another*[212] it was surprisingly that the assessment of authenticity and integrity was determined during judgment writing after the exhibit was admitted while authenticity and integrity ought to be determined at the admission stage.

There are several challenges that can be made to the authenticity of digital records in relation to identity management Challenge which confront our courts and bring misunderstanding between weight and admissibility of evidence: who is the author of the records? Whether a message, document, video, or photo was included in an email or posted on a website, it is important for the proponent to provide testimony about who the author is. Is the Computer Program that generated the records reliable? Was the output of the computer what it is purported to be? Were the records altered, manipulated, or damaged after they were created? Changes to photographs and videos can be made using photoshop or graphic design programs, while hackers can alter websites, change databases, and other electronic media. Often, they cover their tracks by changing audit log records.

The solution to such challenge is that issues of integrity to the electronic evidence are of essence in authenticity of electronic evidence as they may not affect admissibility but rather the weight of evidence. In a challenge to the authenticity of email transcripts, "instant messages," and "chats," a court in a case of *U.S. v. Lebowitz*,[213] held that "obvious omissions" in some of the communications go to the weight rather than the admissibility of the evidence.

[212] Civil Case no. 7 of 2019, High Court of Tanzania at Moshi (Unreported
[213] 647 F. Supp. 2d 133 (N.D. Ga. 2009)

To guide litigants, lawyers and the court on the features of electronic evidence to be admitted into legal proceedings, the legislature in Tanzania set the law showing criteria for determining admissibility and the weight of such evidence.[214] (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.

4.2.4 Absence of Authentication Procedure in admissibility of Electronic Evidence: The Authentication Rule Issue

The authentication procedure, which is designed to indicate the credibility of evidence has vital significance in deciding admissibility and weight of evidence because only evidence with credibility can be admitted and the possibility of credibility decides weight.[215] Authenticity simply means that the content of a document is indeed what is claimed to be hence authentication entails what is the document, where did the document come from and who or how was it created.[216] The process involves the means which the document is verified and examined, its accuracy and formalities observed in the execution of a document. In other way authentication can be termed as the integrity of a document.[217]

In Tanzania, the legislature introduced important changes of recognition to the admissibility of electronic evidences to the Tanzania legal systems;[218] however the changes have minimal application to civil proceedings as they deal with only when

[214] ETA section 18(2)
[215] Tegamaisho P.P(n.26) p.9
[216] Ibid
[217] Ibid
[218] See section 78A and 76 of TEA.

the evidence in the baking business is at issue but not in other transactions or communication like emails etc. Besides in both types of proceedings the Amendments and the new Electronic Transaction Act, 2015 did not stipulate the comprehensive safeguards or procedure for authenticity of electronic evidence. The rules on conditions for the admissibility of electronic evidence in ETA are insufficient and this implies that the general rules of admissibility of evidence such as relevance, authentication and originality codified in TEA continue to apply.

Applying the traditional rules squarely in this era of cyber space without modifications by law makers results into paradoxes and inconsistencies by judges and magistrates. This is because ETA[219] puts admissibility of electronic evidence on equal footing with paper-based evidence. To show that our new digital laws are insufficient, the amendment on TEA talks on admission of electronic evidence in bankers' books together with affidavits from bank officers or partner of bank sworn before commissioner of oaths to prove or authenticate that the electronic evidence was created in ordinary cause of business.[220]

But the provisions of ETA, a specific law, which stipulates criteria for admissibility of electronic evidence does not talk on evidence on bankers' book neither does the law talk on certificates nor use of affidavits from authenticating authority and there is no such legislated procedure for authenticating electronic evidence neither is there any authority with expert in forensic mentioned to be authenticating authority to both

[219] ETA, section 18(1)
[220] TEA, section 78(2)

under ETA or TEA[221]. However, it appears that ETA has mandated the functions of issuing licences to persons to carry out the obligation of certification to regulator under the ministry responsible for Information and Communication Technology to be designated by the Minister in the published notice in the government gazette but the provision which has never been tested in practice as courts merely demand certificates and affidavits from parties regardless which institutions they come from. This has been left to courts hence the root of inconsistent of decisions.

In *Exim Bank of Tanzania case*[222] which was decided after section 78A was inserted in TEA, it is surprisingly that the court unnecessarily raised the higher criteria of proof inconsistently with the available statutory mode of proof provided in sections 78 and 79 of TEA which requires oral testimony or affidavits but the court required authentication by certificates which is not legislated the position which have been followed by courts though inconsistently. Most probably and precisely, this supports this study on the need to rewrite new rules requiring authentication by certificates as additional safeguards.

Furthermore, in *Simbanet Tanzania Limited vs Sahara Media Group Limited*[223] (supra) the High Court required the authentication by use of affidavit of the deponent to assure the court on the reliability of the emails stored, generated, communicated and maintained in his computer in that the computer that stored and

[221] Reading other provisions of ETA including section 18(2) which talks on criteria for authenticity, there is no requirement of affidavit nor certificates of authenticity to be tendered to court.

[222] Exim Bank(T)Ltd v Kilimanjaro Coffee Company Limited, Commercial case No.29 of 2011, HC (Commercial Division) Dar es salaam (Unreported)

[223] Commercial Case no.2 of 2016 The High Court of Tanzania, Commercial Division at Dar es salaam (Unreported)

maintained such emails could not have been accessed by any other person except by himself in compliance with complied with Section 18(2)(a) and (b) but also with Section 18(4) of the Electronic Transactions Act of 2015.However,it was a different position from the case of *EAC Logistic Solution Limited vs Falcon Marines Transportation Limited* (supra) when interpreting the same section 18(2) the court said that an affidavit establishing the reliability of the manner in which the electronic data message was generated is not a prerequisite for admission of electronic documents.

The High Court said that oral evidence or testimony by the witness in charge of the computer suffices and depends on the electronic evidence to be admitted. The High Court further insisted that filing affidavits and certificates to court is necessary when the person seeking to tender the evidence is not the person in-charge of the computer from which the data message was generated or a party to the chain of custody of the electronic document or device. The court further ruled that where a witness is tendering an email of his own no affidavit is required. The court therefore made its own inventions. Whereas in another High Court Case of *Leonard A. Munghor vs Novart Kaijage Zedekiah (supra)* the use of affidavit and Certificates in authenticating electronic evidence were declared mandatory and the court used the term affidavit and certificates interchangeably as if they mean the same thing contrary to the already cited provisions of the law under Evidence Act.

As hinted already, the requirement of filing certificates is neither legislated under Evidence Act nor under electronic transactions does Act save that TEA mention authentication by affidavit but only in bankers books only and thus possibly in civil

cases only. Therefore, equating affidavits and certificates in authenticating electronic evidence to mean the same thing as the court did in *Leonard A. Munghor vs Novart Kaijage Zedekiah* (supra) was a legal challenge in authentication because the term certificate is not defined under the respective law and there is no prescribed form for such certificate which was declared by the court to be akin with an affidavit. It is on this note the law on admissibility and authentication of electronic evidence, one scholar has described to be incomplete, that the law generally ought to be complete for legal certainty and legitimacy purposes.[224].

As portrayed already in *Ivanna Felix Teri vs Viettel Tanzania Public Limited Company and Another* (Supra) laying foundation of an electronic evidence to be tendered was done during judgment stage after the electronic evidence was admitted where the court ruled out its integrity and authenticity. This is the view taken in *Mungai's case* (supra). That is, admit the data message then test its veracity during evaluation of evidence.[225] *The Exim Bank's case and Mwalongo's case* (supra) portray the second school of thought upon which electronic evidence should not be admitted unless the foundation of the evidence (proven reliability and authenticity of the evidence) has been successful.[226] The interpretation and applicability of ETA on section 18(2) and (3) on laying foundation therefore remain as a challenge during admissibility.

For instance, in India there is a clear provision mentioning a certificate for parties who want to rely on e-mails, websites or any electronic record in civil or criminal to

[224] Ubena.J (n.30),62
[225] Ibid, p.63
[226] Ibid

present together with a certificate at the trial.[227] Similarly, in USA in their Federal Rules of Evidence[228], which has various provisions with a list of examples which satisfy the requirement of Authenticity through number of circumstances. Therein, there is a requirement of producing a Certificate as certifying domestic records of a regularly conducted activity if no testimony of qualified expert or witness or a custodian of evidence and the way experts can give opinion or persons giving testimony can be cross examined and similar issues are legislated, the said certificate must comply to the relevant requirement rule.

As already hinted, in spite of the amendments done in TEA and new enacted specific legislation Electronic Transaction, Act,2015, cases determined by the High Court of Tanzania still depict lot of inconsistences of admissibility of electronic evidences facing Tanzanian courts in determining originality, reliability, integrity and authenticity of electronic evidence to be tendered.

The enactments still do not set comprehensive and exhaustive rules to be consistently applied by courts. Still Tanzanian courts find themselves bound to resort to the rules from other jurisdictions to determine admissibility of electronic evidence. For example, surprisingly, the new amendment of TEA was of no assistance to courts as the court in *Lazarius case* (Supra) borrowed a leaf to the USA

[227] Section 65B of Indian Evidence Act.

[228] See rules: Rule 803(6)(D) of Federal Rules of Evidence. Also see other rules such as 901(b) (1), Rule 901(b)(3), Rule 901(b)(4), Rule 901(b)(5), Rule 901(b)(6)A &B, Rule 901(b)(7)A&B, Rule 901(b)(8)A, B &C, Rule 901(b)(9), Rule 901(b)(10) all under Federal Rules of Evidence in USA. They are exhaustive how electronic evidence can be authenticated. See also the Commonwealth Model Law on Electronic Evidence,2017 which is the work of Commonwealth secretariat. The Model Law draws on the Singapore Evidence Act Section 35 (1), the Canada Uniform Electronic Evidence Act, and the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce. See also Draft Convention on Electronic evidence Article 2(1). The rules of authenticity and best evidence rule on electronic evidence have been modified to quench the technological reality.

case of *Lorraine v Market*,[229] which had set rules of admissibility of electronic evidence and authenticity procedures. Views held by scholars have it that Certificates are therefore self-authentication, will not necessarily need further proof or corroboration unless there are compelling circumstances of doing so[230].However, it is argued that Corroboration is an essential tool for the successful presentation of electronic evidence.

It could be better approach in Tanzania if electronic rules with an appropriate authentication process would be introduced, would have reduced the tendency of the opposing party to object to electronic evidence without grounds, because the magistrates and judges, who lack knowledge and expertise with electronic evidence, can easily be confused when evaluating the credibility and the weight of electronic evidence.

4.2.5 The Flaw of Regarding every Electronic Evidence as Hearsay: The Hearsay Rule Challenge

Hearsay is defined as a statement offered in evidence to prove the truth of the matter asserted.[231] Therefore, hearsay evidence is the statement that is given by the third party other than declaring in proving certain matter before the court.[232] The rule entails that, hearsay evidence, is not admissible unless there is a showing of substantial reliability of the out of court statement can be assumed.[233] Electronic evidence in nature may be regarded as hearsay evidence.[234] However not every

[229] 241 F.R.D 534
[230] Thomson (n.33),5
[231] Tegamaisho P.P(n.26) p.11
[232] Gultan, G, (n.15), p.6
[233] Tegamaisho P.P(n.26) p.11
[234] Teppler, S.W(n.35) p.14

electronic evidence is hearsay.[235]

In determining whether electronic evidence is hearsay evidence or not, an important distinction between computer- generated and computer-stored electronic evidence has to be made.[236] The former cannot be regarded as hearsay evidence but the latter is, the reason is not farfetched as the latter involves human who is the one making that stored information.[237] It is therefore incorrect to deny admissibility of electronic evidence generally by regarding it to be hearsay or subjecting it generally in the hearsay without assessing or determining whether it was computer generated or computer stored electronic evidence.

While we appreciate that hearsay rule continues to apply in electronic evidence like in any kind of evidence, but it is important for one to thoroughly assess the source of electronic evidence otherwise best electronic evidence will encounter higher standard of proof hence denial of its admissibility in the absence of sufficient digital rules of admissibility.[238] Although the court in *Le Marsh case* (supra) rightly admitted the computer print outs of record of baker's book as primary(original)documentary evidence the issue of assessing whether it was computer generated or computer stored to see whether it amounted to hearsay or not was not explored likewise in other discussed cases.

[235] Crossey, N.E (n.3g7), p.560
[236] Ibid
[237] D. R. Mathews, Electronic Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search and Retrieval, Taylor and Francis Group, New York, 2013, p.17.
[238] Section 34B and 34C of TEA recognise admissibility of electronic evidence in civil and criminal matters under the hearsay exceptional rule.

For instance, In England and Wales, evidence is governed by the Civil Evidence Act 1995 for civil matters and the Criminal Justice Act 1988 for criminal matters.[239] Evidence is admissible as long as it is relevant to an issue in dispute, subject to a number of exceptions, such as the Hearsay Rule.[240] The Business Records Exception to the Hearsay Rule applies in England and Wales. At common law, the best evidence rule applies, but this has been modified by the Civil Evidence Act 1995 (Eng) and the Criminal Justice Act 1988 (Eng). [241]

In direct or original evidence rule, the court regards the evidence as hearsay, and therefore not admissible as evidence.[242] The case is not similar for electronic evidence. So long there is no issue as to whether the computer was functioning properly or otherwise there was no misuse, electronic evidence is not subject to the hearsay rule.[243] In other words, such electronic evidence is not regarded as hearsay evidence. Because the law says a document is 'anything in which information of any description is recorded. Digital versions of statements are therefore documents admissible to the same extent as paper-based statements, provided the requirements of form and signature are complied with.[244]

4.3 Conclusion

The thrust of this chapter centred on the challenges of admissibility of electronic evidence in Tanzania context. Since the challenges of admissibility electronic evidence are exacerbated by advancement of technology, the challenges therefore

[239] Stanfield (n.39), p.203
[240] Ibid,204
[241] ibid
[242] ibid
[243] ibid
[244] Ibid

become global issue. In that regard the commonwealth model law of electronic evidence was also reviewed in line with other scholarly works and other countries of the world with best practices and experiences who have dealt with the issue of admissibility of electronic evidence in modern approach. Among other countries the UK and USA are some of the examples where challenges were explored including their modernised digital rules to know the causes of such challenges.

The review shows that there are lot of challenges on admissibility of electronic evidence in Tanzania and under global level. However, there are serious approach adopted through legal frame work designed to curb the said challenges though they differ from one jurisdiction to another. However, despite the discrepancies but there are modern laws to country level and as well regional level such as commonwealth model law which quench the technological realities for issues of admissibility of electronic evidence in modern approach.

The chapter disclosed that there are a lot of technological challenges which have challenged the rules of admissibility of electronic evidence. For instance, among other challenges discussed in this chapter, the major challenge was found to be the rule of originality which was long ago applicable in admissibility of paper-based evidence where its legacy still bounds courts in admissibility of electronic evidence. The said traditional rule cannot be applied today in admissibility of electronic evidence in the advent of technology. Even the laws do not attempt to define what is an origin of the electronic evidence and what is the secondary electronic evidence is.

Generally, it was disclosed in this chapter that there are best methods and experiences that Tanzania can learn from Commonwealth Model law instrument and

other jurisdictions with better laws of admissibility of electronic evidence like USA and UK pertaining admissibility of electronic evidence to mitigate the challenge which is mostly caused by its legal framework. They include enacting privacy and data protection laws so as to balance security and privacy so that electronic evidence collected from Tanzania by another country particularly in criminal matters, may be considered reliable and with integrity hence admissible as per international standard, enacting new digital laws which are ideal to admissibility of electronic evidence in issues of electronic transactions particularly on issues of authentication rule and best evidence rule including manner of tendering electronic evidence, issues of cross examination and proof by certificates from responsible authorities. The next chapter will extract key findings from the preceding chapters in order to answer specific objectives and make a discussion to them in a critical way to craft admissibility of electronic evidence in a technological context.

CHAPTER FIVE

DISCUSSION OF FINDINGS ON ADMISSIBILITY OF ELECTRONIC EVIDENCE

5.1 Introduction

This chapter presents the findings from the analysis of the case law and statutory provisions governing on admissibility of electronic evidence in Tanzania. The research aimed to expose challenges and problems posed by the admissibility of electronic evidence in the Tanzania legal system in the digital environment and further examine whether the letters of law are in line with international standard and other better laws from various jurisdictions. This chapter functions as the base of crafting admissibility of electronic evidence in Tanzania to suit in technological context. It endeavours to expose, with rationale and justifications, what was left by the law which now the courts have found themselves giving inconsistent and uncertain decisions.

5.2 Overview of data sources

The data sources included 17 cases law decisions, out of 17 decisions, 16 were from the High Court and 1 from the Court of Appeal of Tanzania ranging from 2000 to 2022 along with examination of relevant statutory provisions under the Evidence Act, Electronic Transactions Act and Cybercrimes Act and international instruments. About 30 legal texts including books, journal articles, reports ranging from 2012 to 2021 and various internet sources were reviewed to obtain secondary data. Qualitative content analysis was employed to interpret the data.

5.3 Key Findings

5.3.1 Challenges of Admissibility of electronic evidence in digital environment.

The analysis identified significant challenges regarding the admissibility of electronic evidence in Tanzania. Although the Evidence Act was amended in 2007 and supplemented by the Electronic Transactions Act (ETA) and Cybercrimes Act both in 2015, the foundational legal framework remains outdated and primarily focused on traditional physical evidence. The rapid advancement of digital technology has not been adequately addressed by these laws, leading to difficulties in interpreting and applying legal provisions consistently. This inconsistency has resulted in conflicting court decisions, exemplified by the *Fadhili Mbwana case,* where the court set an unnecessarily high standard for admissibility, ultimately excluding relevant electronic evidence and causing societal injustice.

5.3.2 Adoption of the Law in International Standard

Findings indicate that despite some legislative progress in recognizing electronic evidence within Tanzanian law, the rules of admissibility still fall short of international standards. Current laws mainly apply to specific contexts, such as banking, neglecting broader digital communication channels like social media. An illustrative case is *Ivanna Felix Teri vs. Viettel Tanzania*, where a social media-generated photo was dismissed due to the absence of the original image or the camera it came from. The research reveals that Tanzanian laws lag behind global standards, such as the Commonwealth Model Laws on Electronic Evidence. The amendments and new laws lack comprehensive guidelines for the authenticity of electronic evidence, as well as protocols for its collection, preservation, and storage.

The key components emphasized in international standards. The Cybercrimes Act only partially addresses these issues, focusing mainly on criminal proceedings.

Overall, the findings highlight the urgent need for a comprehensive legal framework that aligns with international standards and adequately addresses the realities of digital evidence in contemporary legal contexts.

5.4 A critical Analysis

This section discusses the implication of each key finding in relation to the study questions along with the existing literature.

5.4.1 Challenges of Admissibility of Electronic Evidence in Digital Environment

The implication of the challenge of electronic law in Tanzania being incomplete and inconsistent results to the prevailing legal regime to be challenged by the ongoing fast development of digital technology in unprecedented pace. For instance, the fact that TEA still contains common law rules applied in paper-based evidence which still apply in equal footing with electronic evidence has the implication of diminishing the scope of admissibility of electronic evidence or results into the court neglecting to admit evidence which ought to be admissible or vice versa and therefore causing injustice.

Scholars argue that authenticity of evidence was bound by its primitiveness, and the concept of original played an important role in deciding authenticity but today the concept of original cannot be applied to electronic evidence in the same manner as paper-based evidence.[245]

[245] Liu.B., (n.31),39

As legislators and practitioners put much emphasize to original items it is therefore not hard to conclude that it is a preference for original physical items which acts as admissibility standard.[246]Going with the trend of requiring electronic evidence to be submitted with the original physical evidence we will be missing a point on the definition of original electronic evidence as telling the difference between the original physical and copy of electronic evidence is a problem itself.[247] Whereas, in August, 1998, the Scientific Working Group on Digital Evidence defined original digital evidence as physical items but includes all digital data in whatever form.[248] By this definition, it can be grasped that the range of electronic evidence is not limited to those with original physical items but includes all digital data in whatever form.

This study has therefore come with the findings which are alarming that electronic evidence should be treated differently from traditional paper-based evidence due to its ephemeral nature and characteristics because under electronic evidence, it is not possible to say which one is the original or how many originals exist. Therefore, the physical item of storage is just part of the original electronic evidence. It is therefore argued that the traditional standard for original and their copies do not apply in the digital world.[249]

The insufficiency and inadequacy of TEA and ETA lacking laws which guide collection, storage and transmission of electronic evidence deprives the Court to admit electronic evidence which is well authenticated since the data from scholarly

[246] ibid
[247]ibid
[248] ibid
[249] ibid

works disclosed that the rules of admissibility of electronic evidence should start from collection, preservation or storage to the final stage of presentation to court for admissibility purpose.[250] The rules which are stipulated under the CCA are insufficient as they only cover criminal proceedings hence the electronic evidence in Civil proceedings was left unguided, a cause which exacerbate challenges during admissibility of electronic evidence.

With the available legal framework of rules on admissibility of Electronic Evidence in Tanzania being scattered in different legislations which are mixed to both traditional and technological environment becomes hard for courts to interpret and read them harmoniously and homogeneously and hence the result of inconsistent application. This was clearly revealed in *Fadhili Mbwana vs Raymond William Komba* (supra) where the court invoked many provisions from TEA and mixed up with section 18 of ETA and thus raised a higher standard of admissibility of electronic evidence which ended up to expunge the well admitted print out. The implication is that the most useful evidence with probative value may end up being rejected and hence a cause of injustices.

Treating electronic evidence as hearsay evidence without categorising whether the evidence is computer generated or computer stored evidence results to the tendency of neglecting to admit electronic evidence or if admitted becomes vulnerable of being accorded little weight while from scholarly work, it was found that not every electronic evidence is hearsay. In determining whether electronic evidence is hearsay

[250] Guidelines and explanatory memorandum on Electronic Evidence in Civil and Administrative Proceedings adopted by the Committee of Ministers of the Council of Europe on 30 January 2019, p.21-22

evidence or not, an important distinction between computer- generated and computer-stored electronic evidence has to be made. [251] The former cannot be regarded as hearsay evidence but the latter is, the reason is not farfetched as the latter involves human who is the one making that stored information.[252]

The Misunderstanding of the difference between admissibility and weight of evidence by Courts. The finding yields that this study is exacerbated by lack of knowledge to judges, magistrates and advocates. It is argued that physical evidence or paper documents can be forged, and the witnesses' competence can be questioned due to their youth or perceptive defects but all these elements would affect the weight of evidence and not the capability of giving evidence.[253]For instance, it was surprising that in *Fadhil Mbwana's case (supra)* the issue of authentication and integrity was mixed up with the concept of weight of electronic evidence. The implication is to reject admission of electronic evidence on ground of its weight at the admission level the exercise which ought to be done at the evaluation and judgment stage.

The study yielded that The Electronic Transactions Act is the specific law determining reliability, admissibility, authenticity and assessing weight of data message and section 18 of the same law prohibits any rule of evidence to be used to deny admissibility of electronic evidence in any legal proceedings which is the confusion as TEA contains the rules on admissibility of electronic evidence and is

[251] Gardiner, &T. Anderson, Criminal Evidence: Principles and Cases, Cengage Learning, New York,2012,202
[252] ibid
[253]Liu.B (n.31),40

the principal Act. But again, this implies that the rules in ETA are more inclusionary than exclusionary which is likely to allow evidence which ought not be admissible to be admitted and hence causing injustices.[254]

The challenge of having no sufficient rules with comprehensive authentication procedure in admissibility of electronic evidence to accord protection safeguard denies the electronic evidence its credibility which results in failure by the Court in deciding admissibility and weight of evidence. This also finds its support from scholars that only evidence with credibility can be admitted and the possibility of credibility decides weight.[255] . The process involves the means which the document is verified and examined, its accuracy and formalities observed in the execution of a document. In other way authentication can be termed as the integrity of a document.[256]

5.4.2 Adoption of the Rules of admissibility in international standard and other better laws from other jurisdictions.

In Tanzania, the legislature introduced important changes of recognition to the admissibility of electronic evidences to the Tanzania legal systems, however, the study yielded that the changes have minimal application to civil proceedings as they deal with only when the evidence in the baking business is at issue but not in other transactions or communication like emails, WhatsApp, Instagrams etc .This implies that the law is lagging behind the technology and not in line with international standard like Commonwealth Model Laws on Electronic Evidence and other better

[254] Makulilo. A. B, (n.25,)122
[255] (n.25) ,9
[256] ibid

laws like USA and UK model. This is so because both types of proceedings the Amendments and the new Electronic Transaction Act,2015 did not stipulate the comprehensive safeguards or procedure for authenticity of electronic evidence.

The rules on conditions for the admissibility of electronic evidence in ETA are insufficient and this implies that the general rules of admissibility of evidence applied in traditional paper-based evidence in TEA such as relevance, authentication and originality continue to apply. Applying the traditional rules of authentication squarely in this era of cyber space without modifications by law makers results into paradoxes. This is because section 18(1) of this Act in general context puts admissibility of electronic evidence on equal footing with paper-based evidence. The provision is not so exhaustive to cater digital demands hence it is still challenged with technological digital divide.

The finding that section 78(2) of TEA as amended alone talks on admission of electronic evidence in bankers' books together with affidavits from bank officers or partner of bank sworn before commissioner of oaths to prove or authenticate that the electronic evidence was created in ordinary cause of business, while section 18(2)of ETA,a specific law, which stipulates criteria for admissibility of electronic evidence is silent, is an indication that our laws are not adopted to international standard and. This implies that the duty has been left to courts hence the root of this paradox of decisions. As was exemplified in *Exim Bank of Tanzania case* (supra).Th finding which supports this study's findings on the need to amend the existing laws including requiring authentication by certificates as additional safeguards to modernise our laws to align with international standards and other better laws as was

seen in USA authentication laws.

At the international level, the legal frame work of Commonwealth Model law on electronic evidence which is the work of commonwealth countries to guide its member countries to enact modern rules as separate legislation of admissibility of electronic evidence to quench thirsty of digital environment especially on rules of authentications and best evidence should be adopted as there is mandatory provision of Authenticity in modern approach. Moreover, in India where section 65B of India for parties who want to rely on e-mails, websites or any electronic record in civil or criminal to present together with a certificate at the trial.[257] Though the law is not binding in Tanzania but in Nigeria there is a law regulating format and content of certificates just is the case in USA the aspect which lacks in Tanzanian laws and its implication is the result of legal challenge which affects admissibility of electronic evidence.

To show that the legal regime is not in line with international standard and other better laws. In spite of amendment done in TEA and new specific legislation Electronic Transaction, Act,2015, the findings indicate that cases determined by the High Court of Tanzania depict lot of inconsistences of admissibility of electronic evidences facing Tanzanian courts in determining originality, reliability, integrity and authenticity of electronic evidence to be tendered. The enactments still do not set comprehensive and exhaustive rules to be consistently applied by courts. Still Tanzanian courts find themselves bound to resort to the rules from other jurisdictions

[257] (n.38),36

to determine admissibility of electronic evidence.

It could be better approach in Tanzania as by introducing electronic evidence itself, an authentication procedure requires the proponent to present other collateral evidence to support the authenticity of electronic evidence to be in line with internation standard the aspects which lacks in Tanzania. However, the study noted that the digital laws of Tanzania do not talk on corroboration of the electronic document. Without an appropriate authentication process in Tanzania, and the tendency of the opposing party to object to electronic evidence without grounds, the judges, who lack knowledge and expertise with electronic evidence, can easily be confused when evaluating the credibility and the weight of electronic evidence.

For instance, it was disclosed in this study that there are crucial questions confronting lawyers and courts the confusion as shown from case law whether authentication should be proved by filed affidavit or certificates and if is affidavit who should file it and, if is the certificate how many certificates to be filed. Moreover, what should be the format and content of such certificate and finally who should certify it and for which type of evidence? For instance, in the case of *EAS Logistic Solution Ltd vs Falcon Said* (supra) the High Court said that Affidavit establishing reliability of the manner in which the electronic data message was generated, stored, communicated, maintained and the original identified is not prerequisite for admission of electronic documents.

However, though under section 33 of ETA it is provided that the Minister may by notice published in the Gazette, designate a government institution under the

Ministry responsible for Information and Communication Technology to be a regulator of Cryptographic and certification services.[258] Upon which the regulator among other functions will be mandated to license and regulate certification services, to determine standards to be maintained by certification authorities as well as to keep and maintain a register of certification services.[259]

The fact that in Tanzania law provides for the admissibility or the handling of electronic evidence without involving digital evidence professionals or to bring them as witnesses in the trial involving electronic evidence, results to believe a layman in adducing electronic evidence without expertism which the court becomes not properly assisted as not all witnesses are the trained operator of the machine (computer driven device).

For example, 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. 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.[260] This helps to avoid a naive 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

[258] ETA, s.33
[259] ETA, s.34(a)(c)(d)
[260] 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), 119 see Chapter 6 in particular for examples.

lead to system failure, inaccessibility of the system-controlled services or an error in the electronic records.[261] 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.

5.3 Conclusion

The analysis of the legal framework of admissibility of electronic evidence in the advent of technology has disclosed serious omissions and inadequacies concerning the electronic laws on admissibility of electronic evidence in Tanzania. There are lot of challenges which are caused by both legal and lack of knowledge in the cyber space which is exacerbated by rapid development of technology. Our laws are lagging behind the technological developments. The Evidence Act, The Electronic Transactions Act and Cyber Crimes Act of Tanzania remains to be the particular law that regulate the admissibility of electronic Evidence. The Evidence Act when was enacted its rules did not contemplate the digital environment since its rules regulated admissibility of traditional paper-based evidence. The Evidence Act, despite its amendments has portrayed clearly that some provisions are unworkable despite being well construed in the Act. This situation is accompanied by lack of clarity as some provisions contradict each other and are still bound by the elements of traditional paper-based evidence which do not apply in digital environment of admissibility of electronic evidence.

[261] Ubena, p.8

Despite of the legislature to enact ETA as an electronic law to complement TEA but still portrayed that its provisions are insufficient and incomplete in a sense that when applied by Courts reveal inconsistences and uncertainties to the great extent of causing injustices. Its provisions contradict with those of TEA. The laws have no comprehensive safeguards for governing authenticity of electronic evidence to be harmoniously and homogeneously applied. Proper and comprehensive rules of authentication in admitting electronic evidence is needed so that uncertainties in electronic evidence be ruled by the authenticity which in turn the court may fairly decide on weight of evidence after admissibility.

CHAPTER SIX

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

This chapter provides summary of findings, conclusion and recommendations. It serves succinctly to present key outcomes of the research, interpret their significance and suggest practical actions or further areas for exploration.

6.2 Summary of Findings

Precisely, this section summarizes the critical findings from the research on the admissibility of electronic evidence within Tanzania's legal framework. The analysis revealed significant challenges and inadequacies in the existing laws and practices, as highlighted in Chapter Five.

6.2.1 Legal Challenges

The Evidence Act, despite its amendments and the introduction of the Electronic Transactions Act (ETA) and the Cybercrimes Act, has not effectively adapted to the digital environment. The traditional principles of admissibility continue to prevail, creating inconsistencies in court rulings and often leading to unjust outcomes.

6.2.2 Inadequate Legislative Framework

The current laws do not sufficiently address the collection, preservation, and authentication of electronic evidence. This has left the courts without a clear procedural basis for evaluating electronic evidence, leading to the rejection of potentially critical evidence due to procedural ambiguities.

6.2.4 International Standards

The rules governing the admissibility of electronic evidence in Tanzania lag behind international standards. Key provisions found in international frameworks, such as the Commonwealth Model Law and practices in jurisdictions like the USA and UK, have not been fully adopted or implemented in Tanzania, further complicating the legal landscape.

6.2.4 Inconsistent Judicial Interpretations

The research found that inconsistent interpretations by judges regarding the admissibility and weight of electronic evidence have resulted in significant legal uncertainties. Notably, cases such as *Fadhili Mbwana and Ivanna Felix Teri* highlighted the lack of clarity in distinguishing between hearsay and admissibility standards, which undermines the integrity of judicial proceedings.

6.2.5 Need for Expertise

There is a marked absence of expert input in the legal process concerning electronic evidence. Judges and legal practitioners often lack the technical expertise needed to assess electronic data appropriately, leading to potentially erroneous decisions.

6.3 Conclusion

The study concludes that Tanzania's legal framework for the admissibility of electronic evidence is outdated and inconsistent, creating barriers to justice in the digital age. The legal framework is not in line with international standard and other better laws from jurisdictions who have gone far ahead. The failure to establish comprehensive rules for the handling and authentication of electronic evidence

results in significant legal challenges, including the risk of injustice due to the rejection of relevant evidence. Moreover, the legislative efforts to modernize the laws have not adequately kept pace with technological advancements, further complicating the ability of the courts to address digital evidence effectively. As the digital landscape continues to evolve, it is imperative that the legal framework in Tanzania adapts accordingly to ensure the fair administration of justice.

6.4 Recommendations

Based on the findings and conclusions drawn from the research, and, in order to address the discussed challenges and ensure that there is a fair trial in the administration of justice, it is recommended by addressing to the respective institutions and stakeholders as follows:

Comprehensive Legislative Reforms: There is an urgent need for a complete overhaul of the legal framework governing electronic evidence in Tanzania by the Legislature. This should include the enactment of specific legislation that addresses the unique characteristics of electronic evidence, incorporating comprehensive rules for its collection, preservation, and authentication.

Adoption of International Standards: The Tanzanian legislature should adopt international best practices, such as those found in the Commonwealth Model Law on Electronic Evidence and relevant provisions from jurisdictions like the USA and UK. This will provide a solid foundation for consistent and fair judicial proceedings concerning electronic evidence.

6.4.6 Training and Capacity Building

Judicial officers, legal practitioners, and law enforcement personnel should undergo training to enhance their understanding of electronic evidence and related technological issues. This will empower them to make informed decisions regarding the admissibility and evaluation of electronic evidence.

4.4.7 Expert Testimony in Court

Courts should establish protocols for the involvement of digital evidence professionals in proceedings involving electronic evidence. Their expertise is crucial in ensuring that the evidence presented is properly understood and evaluated.

4.4.8 Public Awareness Campaigns

Stakeholders, including legal practitioners and the general public, should be educated by the government on the significance of electronic evidence and the legal processes surrounding its admissibility. Increased awareness can foster greater compliance with legal standards and practices.

4.4.8 Regular Review and Updates of Legislation

The legal framework must be reviewed regularly by institutions like the Tanzania law reform commission to ensure it remains relevant and effective in addressing the challenges posed by evolving digital technologies. This proactive approach will help mitigate the risks of outdated laws leading to injustices in the future.

By implementing these recommendations, Tanzania can move towards a more robust and equitable legal system that effectively accommodates the complexities of electronic evidence in the digital era.

BIBLIOGRAPHY

Anand, A, et al, *The Supreme Court of India re-defines admissibility of electronic evidence in India*, Digital Evidence and Electronic Signature Law Review, 2015, 12.

Bo Liu, *Problems on the admissibility of electronic evidence in the Chinese Context*, Digital Evidence and Electronic Signature Law Review, 2015,12,

Crossey, N.E, *Machine Translator Testimony & the confrontation Clause: Has the time come for hearsay rule to escape from the Stone Age*? Drexel Law Review, 2020, Vol. 12, 561.

C. Nemeth, Law and Evidence: A primer for Criminal Justice, Criminology, Law and Legal Studies, Learning, London,2012,141

Gardner, & T. Anderson, Criminal Evidence: Principles and cases, Cengage Learning, New York, 2012

Gultan, G, Privacy Concerns relating to the collection of electronic evidence: under Turkish legal system and cybercrime convention, Master Thesis, Faculty of Law University of Oslo, (n.y)

Hait A.A, *Jurisdiction in Cybercrimes: A cooperative study*, Journal of law policy and globalization, 2014, Vol.22, No. 2224-3240

Institute Company Secretaries of India, Cybercrime law and Practice., New Delhi: Samrat Offset Works,2016

Jonathan, C., *A world of Differences: The Budapest convention on Cybercrime and Challenges of harmonisation*, Monash University Law Review, (N.Y) Vol.40, No.3

Mrema, K.J, Piercing the corporate veil of group companies: A critical legal analysis

under the companies Act of Tanzania, A LLM dissertation, The Open University of Tanzania, Dar es Salaam, 2020.

Nikolaus Forgó, Christian Hawellek, Friederike Knoke, and Jonathan Stoklas, 'Privacy Protection in Exchanging Electronic Evidence in Maria Angela Biasiotti and others (eds) Handling and Exchanging Electronic Evidence Across Europe, Law Governance and Technology Series 39, 2018. 256.

Kiunsi, H. Transfer Pricing in East Africa: Tanzania and Kenya in comparative perspective, A PHD thesis, Open University of Tanzania, 2017.

Kulehile.M. R, Analysis of the regulatory principles of functional equivalence and technology neutrality in the context of electronic signatures in the formation of electronic transactions in Lesotho and SADC region, a PHD thesis, Department of Private Law, University of Cape Town, August, South Africa, 2017.

Kuner.C., "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future, TILT Law & Technology Working paper No.016/2010 October, Versions 1.0.

Makulilo, A.B, *Admissibility of Computer Evidence in Tanzania*, Digital Evidence and Electronic Signature Law Review, 2007.

Makulilo A.B, *The Admissibility of electronic evidence in Tanzania: new rules and case law*, Digital Evidence and Electronic Signature Law Review,2016,13

Makulilo, A.B 'The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius, 2021.

Mambi, A.B, *Electronic evidence in Tanzania*, Digital evidence and Electronic Signature Law Review, 2013, Vol.10.

Mason, S and Seng, electronic Evidence 4th edn, 2017.

Mason, E*lectronic evidence and the meaning of original*, Amicus Curie 79 Autumn, 2009.

Mathews, D.R, Electronic Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search and Retrieval, Taylor and Francis Group, New York, 2013.

Michael J. Hannon. Digital Evidence-computer forensics and legal issues arising from computer investigations (William S. Hein & Co., Inc., 2012), at 331.

Mkandya, B.H, Admissibility of Electronic Evidence in Tanzania: Law and Practice, A LLM Thesis, Open University of Tanzania, 2011.

Setthapirom, W, The Collection of Electronic Evidence in the Prevention of Cybercrimes A Dichotomy Between Security and Privacy, Orebro University, 2021.

Stanfield, A.R, The authentication of electronic evidence, PHD thesis, Faculty of law Queensland University of Technology, Australia, 2016

Swales. L, *An analysis of the Regulatory environment governing Hearsay Electronic Evidence in South Africa: Suggestions for reforms*, Part two PER/PELJ, 2018 Vol.21-DOI

Tegamaisho P.P, *Authenticity of Electronic Evidence; A comparative analysis between the Position in Tanzania and Kenya*, Ruaha Law Review Faculty of Law Ruaha Catholic University, 2018, Vol. 5-6y, No.1

Teppler, S.W, *Digital Data as Hearsay*, Digital Evidence and Electronic Signature Law Review, 2009, Vol 6,7.

Teppler, S.W, *Testable reliability; Modernised approach to ESI admissibility*, Ave

Maria Law Review,2014, Vol.12.

Thomson, L.L, *Mobile Devices, New challenges for Admissibility of Electronic Evidence*, SciTech Lawyer, 2013, Vol 9, 3.

Ubena, J., Guiding notes on tendering and admissibility of electronic evidence in Tanzania, 1st Ed, Tanganyika Law Society, Dar es salaam, 2020.

Ubena.J, *Legal issues surrounding the admissibility of electronic evidence in Tanzania*, Digital Evidence and Electronic signature Law Review, 2021, Vol. No.18, 66.

Uchena, J.O, "*The African Union Convention on Cybersecurity; A regional response Towards Cyber Stability?* Masaryk University Journal of Law and Technology, 2018, Vol.12.2.

APPENDICES

Appendix 1: Research Clearance Letter and Manuscript

A: Clearance Letter

THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY

THE OPEN UNIVERSITY OF TANZANIA

Ref. No OUT/PG202000108 **13th July, 2023**

To Whom It May Concern,

RE: RESEARCH CLEARANCE FOR MR.EDWIN MWOMBEKI KAMALEKI, REG NO: PG202000108

2. The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1st March 1993 by public notice No.55 in the official Gazette. The Act was however replaced by the Open University of Tanzania Charter of 2005, which became operational on 1st January 2007.In line with the Charter, the Open University of Tanzania mission is to generate and apply knowledge through research.

3. To facilitate and to simplify research process therefore, the act empowers the Vice Chancellor of the Open University of Tanzania to issue research clearance, on behalf of the Government of Tanzania and Tanzania Commission for Science and Technology, to both its staff and students who are doing research in Tanzania. With this brief background, the purpose of this letter is to introduce to you **Mr. Edwin Mwombeki Kamaleki, Reg.No: PG202000108),** pursuing **Master of Law in Information and Communication Technology (LLMICTL).** We here by grant this clearance to conduct a research titled **"The Advent of Technology and Its Challenges on the Rules of Admissibility of Electronic Evidence: Do We Need Further Legal Reforms".** He will collect the documentary review from 14th July 2023 to 21st September 2024.

4. In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O.Box 23409,

Dar es Salaam. Tel: 022-2-2668820.We lastly thank you in advance for your assume cooperation and facilitation of this research academic activity.

Yours sincerely,

THE OPEN UNIVERSITY OF TANZANIA

Prof.Gwahula Raphael Kimamala

For: VICE CHANCELLOR

Kinondoni Biafra, Kawawa Road; P.O 23409; Dar es Salaam; Tel: +255 22 2668 445;
E-Mail:vc@out.ac.tz|| Website:www.out.ac.tz