Page 340 - 351 **DOI:** *https://doij.org/10.10000/IJLMH.118117*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 5

2024

Analysis of Digital Evidence Admissibility in the Administration of Justice in Kenya: An Implication of Sexual Offenses Crime

JOANES OFWA[1]

ABSTRACT

Digital evidence just like other forms of evidence are expected to provide information to court trying cases, involving factual disputes including testimony, documents, and physical objects Section 3(2) of the evidence Act CAP 80 of the laws of Kenya, defines evidence as something (including testimony), documents and tangible objects that tend to prove and disprove existence of the alleged facts. In the words of Eughan Cassey, digital evidence is "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as an intent or an "alibi". This paper focuses on the substantive laws providing the legal frame works for the admissibility of digital evidence in the administration of justice in Kenya with emphasis on sexual offenses cases. The paper intends to analyze the adequacy and the effectiveness of Kenya laws when handling digital evidence in the administration of justice. The object of a court is to administer justice and the purpose of digital evidence investigators is to present or provide supporting evidence, facts, and the probabilities. The fundamental question, should any digital evidence stored in a computer continue to be treated as documentary evidence? It is imperative to examine the jurisprudence from other jurisdictions as well. The paper analyzes whether digital evidence is admissible in Kenya and its consideration of probative value and reliability.

***Keywords**: Relevance, admissibility, evidence, probative value, electronic evidence.*

I. INTRODUCTION

Dictionary of Criminal Justice defines evidence as [2]"*All means of giving information to court trying cases, involving factual disputes including testimony, documents and physical object. In English common law system, the law of evidence principally determines when to admit or exclude evidence items"*. **Section 3(2) of the Evidence Act Cap 80**[3] determines evidence "The means by which an alleged fact is proved or disproved …or being perceived by the senses and

[1] Author is a Lawyer & PhD Scholar at School of Business and Economics, Jaramogi Oginga Odinga University of Science &Technology, Kenya.
[2] Dictionary of criminal justice 7th Edition, California State University, Long Beach
[3] The evidence Act CAP 80 of laws of Kenya

 [ISSN 2581-5369]

any mental condition of which any person is conscious." Blacks law dictionary[4] *defines evidence as 'something (including) testimony documents and tangible objects) that tends to prove or disprove the existence of an alleged fact. (The bloody glove is the key piece of evidence for prosecution. The collective mass of things especially testimony and exhibits presented before a tribunal in a given dispute'.* The evidence will show that the defendant breached the contract.")

Eoghan Casey in his book digital evidence and computer[5] defined digital evidence as "*any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that addresses critical elements of the offense such as intent or alibi."* The data is basically the combinations of various symbols, numbers that contain diverse information such as texts, images, audio, and video. Digital evidence has been defined by different scholars but do not agree that it is any data that is capable to establish the occurrence or existence of a crime as committed by the persons linked to it. (Casey, 2000)

The standard working group in Digital evidence (SWGDE) do propose that any information of *probative value* which is better stored or transmitted by a device in a digital form constitutes a digital evidence. The other definition comes from the Association of Chief Police Officers[6] that digital evidence is information and Data of investigation value that are stored on or transmitted by a computer. While Carrier (2006),[7] asserts that digital evidence, is a digital data that may support or refute a hypothesis about any digital event or the state of affairs where digital data is stored or transmitted by a computer.

According to Henselar (2000),[8] the sources of digital evidence can be categorized into three computer systems groups;

First is an *open computer system*, it comprises hard drives, keyboards and monitors such as laptops, desktops and servers that obey standards. There is an increasing trend of the amount of storage space which can be a rich digital evidence. There may be a single file containing incriminating information and can have an associated property that are useful in an investigation. For example, the details such as when a file was created, who most likely created it, or that it was created on another computer can all be important.

The second *communication systems.* The traditional telephone systems, wireless

[4] Blacks Law Dictionary,9th edition 2009, West Publishing Company
[5] Digital Evidence and computer crime (forensic, Science, computers and the internet)
[6] Ibid
[7] Brian Carrier (2006)
[8] Henseler (2000) foundations of Digital forensic

 [ISSN 2581-5369]

telecommunications, the internet and the networks in general can be a source of digital evidence (electronic evidence). The telecommunication system transfer sms/mms messages and internet carry email messages globally. The investigation can reveal for example the time a message was sent, who likely sent it or what the message contained. Too verify when a message was sent or data input can easily be examined from the log files from the immediate server and routers that handled a given message.

The third *embedded computers system*s. The mobile devices, Visa Cards, Master Cards or other Cards with electronic chips and many other systems with embedded computers may contain digital evidence. For example, Navigation systems can be used to determine a vehicle speed at the time of accident, brake status and throttles position during the last five seconds. (5s) before the impact in an accident. In an arson, investigation, data recovered from a microwave oven can indicate that it was strategized to trigger a fire at a specific time.

It should be noted that electronic or digital data should be collected routinely in any investigation. More often than not, a suspect involved in a crime must have operated a computer, used a mobile device or accessed the internet, therefore a case where a corporation or an organization is supposed to be investigated, the investigator should consider information which are relevant and stored on a computer system used by their employees both at work and at home. Every search warrant should include digital evidence in order to save time by issuing a second warrant.[9]

(A) Statement of the problem

The object of a court of law is to administer justice and the purpose of digital/ electronic investigators is to present or provide supporting evidence, and facts and probabilities of the occurrence of the claims being pursued in court of laws.There is a problem with digital evidence in cases where the investigator comes across incriminating evidence in plain view but not covered by the search warrant such as child pornography and other sexual offenses.Criminals may attempt to destroy digital evidence by wiping or destroying devices consequently making it hard for the forensic investigators to gather the evidence resulting to seek the services of a specialists in decryption tools and techniques.

(B) **Objective of the study:** To analyse digital evidence admissibility in the administration of justice in Kenya: an implication of sexual offenses crime

[9] Ibid

 [ISSN 2581-5369]

(C) **Hypothesis of the study:**There is no significant effect of digital evidence admissibility in the administration of justice in Kenya.

(D) Methodology and Literature review

a. Research design

Desk top design is adopted because the constitution, statutes and cases are examined supported by contents obtained from online articles and journals rather data gathered from field survey.Desk research methodology is a method of collecting and analyzing information from available secondary sources, such as documents, reports, academic publications and other materials available online or in libraries.(John W. Creswell and J. David Creswell[10])

(E) Literature review

a. Theoritical review;Panopticon theory

The study is anchored on panopticon theory which was advanced by Jeremy Bentham in the 18th century, It was an architectural design that could be used for prisons, schools, factories workhouses and any other such institutions that required the system of managing a large group of people by a small group of individuals with enormous authority.[11] although it is often argued that Bentham's model has never been realized, several prisons are constructed according to the broad principles of panopticism. Where a circular building with individual cells erected around its entire circumference, and a central watchtower in which the activities of the prisoners could be constantly monitored. A system of lighting that illuminated the cells but kept the watch tower in darkness made it possible for just one person to check on many inmates, each of whom knew they were under surveillance[12].

Western societies have experienced a rapid growth in the use of surveillance[13], in the last 15 years to the extent that most citizens have not taken for granted that they are being observed, monitored, classified and controlled in almost every aspect of their public lives. Closed Circuit Television (CCT) is in the forefront of the surveillance society[14], on average people living and working in the major cities are usually filmed up almost 300 times a day (Norris,2003)

Electronic evidence provides a new dimension in investigation, because every crime to some extent has an associated data stored in the computer and transmitted using a computer system.

[10] John W. Creswell and J. David Creswell Research design Qualitative and Quantitative and mixed methods approaches 2017)
[11] (Coleman and Norris,2000)
[12] ibid
[13] Norris (2003)
[14] Ibid

 [ISSN 2581-5369]

In fact, an individual's personal computer and, his use of network services are effectively a behavioral archives and may potentially retaining, more information about a person's activities and his/ her desires than the family member.

II. ADMISSIBILITY OF DIGITAL/ ELECTRONIC EVIDENCE

After looking at the fundamental purposes and roles of computers in crime when dealing with digital evidence. It is imperative to focus on the admissibility of electronic evidence. Admissibility of evidence is a matter in law which judicial officers have to determine. As a general rule, all evidence of sufficient relevance to prove or disprove a fact is in issue admissible.[15] Under section 3 of Kenya Evidence Act the term '*Admissible*'[16] means admissible in evidence, meaning evidence presented in court and what it may consider before the determination of a case. In the words of Casey[17], 'the Law and scientific knowledge to which it refers often serve different purposes concerned with ordering men's conduct in accordance with certain standards, values, and societal goals' The legal system is a prescriptive and normative one, dealing with the 'ought to be'[18] much scientific knowledge, on the other hand, is purely descriptive; its laws seek not to control or judge the phenomenon of the real world, but do not describe and explain them in neutral terms.[19]

The object of a court room is to administer justice and the purpose of digital/ electronic investigators is to present or provide supporting evidence, and facts and probabilities, therefore the court depends on the truthful investigators and their capacity to provide technical evidence accurately. Since courts are concerned with the authenticity of the digital evidence, the electronic investigators are expected to be honest and forth right and the evidence must meet the expected standards to be admitted. A mere saying that 'a glove was found in suspect's home 'is not enough but it is another matter to prove it. Therefore, when guilt or innocence hangs in the balance, the proof that evidence is authentic and has not been tampered with becomes essential. The roles of evidence is that, before admitting it,a court must ensure that it is relevant, and evaluate the evidence to determine if that is what proponent claims, if the evidence is hearsay, if it is unduly prejudicial and if 'the original is required or the court will admit the presented copy as being sufficient evidences.

The admissibility of the electronic evidence may require the duty of experts. Generally, experts

[15] Kyalo Mbobuthe law and practice of evidence in Kenya, law Africa publishing (K) Ltd
[16] Ibid
[17] Digital Evidence and computer crime (forensic, Science, computers and the internet)
[18] ibid
[19] Ibid

 [ISSN 2581-5369]

have a duty to present the objectives, unbiased truth on the matter before the court. Experts are restrained to advocate for one side or support one party knowingly or willingly.[20]

The UK criminal procedure rules (CPR) address specific issues concerning Experts Statements as follows[21]

i. An expert must help the court to achieve the overriding objectively by giving objective, unbiased opinion on matters within his expertise.

ii. This duty overrides any obligation to the person from whom he receives instructions or by whom he is paid.

iii. The court and all the parties should be informed if there is any change on the experts

In Kenya the law recognizes electronic or digital evidence, providence it conforms to the required threshold prescribed by the written laws especially as provided for in *section 106B of the evidence Act.* While courts in Kenya take cognizance of electronic evidence, they are not accepted and admissible automatically, unless the evidence has been subjected to an authentication by an expert. **Civil Suit 31 of 2014(OS). On the 9th June 2016**, the defendant in the suit for the sharing of the matrimonial property, sought to play the audio record, it was objected by the plaintiff by citing section 106B (4) of the evidence Act Cap 80, law of Kenya, which requires that the kind of evidence ought to be accompanied by *a certificate,* and that the certificate must identify the electronic record that is containing the statements and details that was used to record the conversation.

Section 106B (4)[22] of the evidence Act states as follows:

"in any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following"[23]

a) Identifying the electronic record countering the statement and describing the manner in which it was produced.

b) Giving such particulars any device involved inn the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a company.

c) Dealing with any matter to which conditions mentioned in subsection(2) relate and

[20] Digital Evidence and computer crime (forensic, Science, computers and the internet)
[21] Ibid
[22] The evidence Act CAP 80 of laws of Kenya
[23]The evidence Act CAP 80 of laws of Kenya

 [ISSN 2581-5369]

d) Purporting to be signed by a person occupying a reasonable position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) or the management of relevant activities (whichever is appropriate)

Shall be evidence of any matter in the certificate and for the purpose of this subsection for a matter to be stated to the best of the knowledge of the person stating it "The provisions of section 106B have been subjected to a number of tests as captured in diverse law cases in Kenya. *In Republic Vs Barisa* Wayu Matuguda (2011)eKLR[24], where electronic evidence was a compact disc(CD) was lifted from CCTV footage, and the court held that whenever any information of substance is stored in a digital device namely computer such as CCTV camera and later produced or copied to the optical device like a CD, then there would be treated as documentary evidence and is admissible. Judge Musyoka observed that "*Any information stored in a computer… which is then printed or copied shall be treated just like documentary evidence and will be admissible without the production of the original".* However, in **William Odhiambo Oduol Vs Independent Election and Boundaries Commission & 2 others eKLR[25].** the dispute was on the admissibility of a video recording performed on a Nokia phone, which was taken to Nairobi and the video recording was then developed to CD. The court observed that the video was recorded, saved in the internal memory of the phone. The phone was connected to a computer using a micro-*USCB* data cable. The file was copied to an empty hard Disk, an empty CD was then inserted into the computer CD with RAM, the file was then written on the CD or VCD using a CD writing applications. It was emphasized that it was imperative to trace the input devices for audit purposes. The court held that the Certificate has to be signal by a person occupying a responsible position in relations to the roles of the relevant device. **In the case of Nonny Gathuri Njenga &Annur Vs Catherine Masitsa and another (2014) eKLR[26],** the decision of the court on admissibility of tape recording was that for DVD to be relied on,[27] '*it must be accompanied by a certificate as required by the section 106B of the evidence Act CAP 80 of laws of Kenya'.*

The court must satisfy itself that the production of the recorded tapes are original as shown *prima facie.* The history of recordings, the productions and the ultimate production in court must meet the threshold of the digital or electronic evidence. **In R *Vs Robson and Harris (1972)[28] 1 WLR 651.***The issue was the admissibility of tape recording of alleged conversation

[24] Republic Vs Barisa Wayu Matuguda (2011)eKLR
[25] William Odhiambo Oduol Vs Independent Election and Boundaries Commission & 2 others eKLR
[26] Nonny Gathuri Njenga &Annur Vs Catherine Masitsa and another (2014)
[27] Ibid
[28] R Vs Robson and Harris (1972)[28] 1 WLR 651[28]

between defendants and a prosecution witness. The court held that' *for a court to make a determination on the admissibility of text telephone conversation the telephone numbers of the persons who were engaged in a conversation must be provided'.* **In Attorney General of Republic of Uganda Vs the East African Law society and another, application No.17 of 2014, the** applicant sought the orders from the East Africa Court of Justice at Arusha, first instance Divisions to be pleased to conduct *a voir dire* in respect to admissibility of the affidavit of Mr. JamesAggrey Mwamu and the electronic Digital Video Disk (DVD) evidence submitted therein filled on the 4th day of March, 2013.The court held that since the prayer had been granted by the *voir dire* proceedings being conducted on 3rd May 2016, the same is now met and that on the issue of admissibility of the DVD evidence would be dealt with when court assessed the totality of all evidence to be presented in Reference No 2 of 2011, and its *probative value in* determination of the sand reference.

Section 84 of the law of evidence Act 2011 in Nigeria provides for the admissibility of computer-generated information or electronic evidence, it has located electronic and computer-generated evidence as part of documentary evidence. ***In Amitabh Bagchi Vs Erick Baghi (2005)[29].*** the court held that physical presence of a person in court may not be mandatory for the purpose of gathering evidence if the same can be done through the use of video conferencing since the definition of electronic evidence include video conferencing. *In* ***the state of Maharashra Vs Dr. Praful B Desai (2003)[30],*** the supreme of India pronounced itself that video conferencing is an advancement of science and Technology which allows seeing, hearing and talking with someone who is not possible to be present physically, therefore the legal requirement for the presence of the witness does not mean actual physical presence.

III. CHALLENGES OF ELECTRONIC EVIDENCE

While the positive properties about electronic evidence can be highlighted such as, it is exact, complete, precise, clear, true, objective and neutral and that electronic evidence appears to be necessary for the resolution of certain type of crimes, it is equally perceived on the other hand as inconvenience in the establishment of legal value. Electronic evidence is perceived difficult due to the existing ignorance about the procedures of data collection, processing and the interpretation of the prosecutor as occasioned by the lack of suitable and systematic regulations and also the lack of homogeneous jurisprudence. There is high chances or degree or volatility of electronic evidence nature, which makes the evidence vulnerable.

[29] Amitabh Bagchi Vs Erick Baghi (2005)
[30] the state of Maharashra Vs Dr. Praful B Desai (2003)

Electronic evidence raises some fundamental questions on legal implication and societal one. In the recent past the media has also been involved in the collection of electronic evidence. The most notable legal issues that electronic evidence has raised in diverse jurisdiction may include:

i. The gathering and production of evidence by means of disclosure.

ii. The issues of admissibility authentications and reliability of the digital evidence.

iii. The issue of interpretation and evaluation of electronically produced evidence including what is captured in the social media.

iv. The infrastructure set ups in various court jurisdiction.

v. The training and retraining of judicial officers

vi. Electronic documents are prone to manipulation by the parties, it hence considered less reliable compared to paper documents. **Zubulake Vs UBS Warburg (2003)** a US Judge stated that [31]"Electronic evidence only complicate matters" it has become easier to interfere or to tamper or delete the document that are maintained electronically.

Concerning the reliability and document integrity in relation to thereto, it is not easy to establish how electronic evidence illegally obtained can be excluded or expunged from the entire evidence records. The use of emoticons and emojis as electronic evidence in a criminal case, has raised a lot of questions whether their use can be interpreted as a threat (e.g angry smiley or guns) or sending/ a threatening text.

*'A teenage from Netherlands was found not guilty in 2010 of threatening the former Dutch Prime minister Jan- Peter Balkenede considering the poorly written text and because he had added smileys'.*There are cases of lack of judicial transparency owing to the complexity in the technology, especially whether the expertise is required and about the privacy. The findings of experts require the proper understanding of the lawyers and the court.

In **Raila Odinga & 5 others Vs. Independent Electoral & Boundaries Commissions & 3 others [2013] eKLR,** Supreme Court of Kenya, the petitioner challenged the legality of IEBC declarations of Uhuru Kenyatta and William Ruto as president elect and Deputy President-elect respectively. The court observed that sections of the Election Act state *"ballot paper means a paper used to record the choices made by the voter and shall include an* ***electronic version of a ballot paper*** *or its equivalent for purposes of electronic voting."* The court drew the conclusions that neither legislature nor IEBC had placed any significant meaning on the *rejected ballot papers* and the ballot paper marked and inserted in to the ballot box has to be considered

[31]Zubulake Vs UBS Warburg (2003)

 [ISSN 2581-5369]

as a *vote*. In an election petition case, the court declined to admit the electronic evidence where a video alleged electronics malpractice was presented, despite the author/ maker / who took the video confirming that he was the one who took the video from his phone. The court stated that the process required a certification as stipulated in Section 106 B of the Evidence Act. [32]The litigants and prosecutors are advised to use and retain the services of a technical expert to assist in production of evidence.

It should be noted that failure to admit electronic or digital evidence is viewed as a miscarriage of justice. When digital evidence is disallowed as part of admissible evidence will grossly impact on the process of administration of justice generally. There are cases of lack of judicial transparency, owing to the complexity of the technology, may derail the litigation process. Storage of evidence and the ultimate production of the required certificates to authenticate the source of the evidence. I am in the view that the mitigation on the challenges on relevancy and admissibility of electronic evidence are within the prerogative of the judicial officers.

IV. RECOMMENDATION AND CONCLUSION

(A) Recommendation

It is a common knowledge that Kenya has a remarkable internet penetrate rate of nearly 90 per cent for the adult population. Today even trade is conducted online through the e-commerce platforms.The judiciary should ensure that emailing of a document and filing of documents should be made simple and user friendly as opposed to the current filing system where a document has to be filed only when the filing system becomes available due to internet availability, which prompts queue of the documents[33].

The electronic exchange of documents among the parties in the litigation, should by hastened by the court systems, process during trial and appropriately use the technology for the purposes of information exchange/ sharing. The electronic signature/ computer tablet signature validity and authentically should be fast tracked by the judiciary by introducing a filter system in order to avoid disputes related to the authenticity, these can be achieved by carrying out the following;

i) The Judiciary to establish and guarantee the homogeneity in the treatment of electronic evidence

ii) *Prevention:* There should a computer protocol to be issued by the companies in the labor relations

[32] Ibid
[33] Gazzete Notice No.2357 practice Directions on electronic case Management

iii) *Training:* The investigators and judicial officers to receive continuous advisory measures to know how electronic evidence can be gathered, produced and stored

iv) *Legislation:* The parliament should design an implementation of protocols that is focused on the protection of fundamental rights during the collection, preservation and presentation of the electronic evidence especially in sexual offenses cases.

(B) Conclusion

On my evaluation of the issues of electronic evidence it is crystal clear that Kenyan laws on admissibility of electronic evidence in court is not sufficient, a lot of improvement is still desirable because various court jurisdictions reach different judgments, when determination of reliability and relevancy of the electronic evidence is disputed.

*****

 [ISSN 2581-5369]

V. REFERENCES

(A) Constitution

- The constitution of Kenya 2010
- Article 50(2) (i) of the constitution of Kenya 2010
- Article 50 (2)(a)

(B) Statutes

- The evidence Act CAP 80 of laws of Kenya
- Section 106B of the evidence Act CAP 80 of laws of Kenya
- Section 118 of the Criminal procedure code

(C) Bibliography

- Eoghan Casey(2000) Digital Evidence and computer crime (forensic, Science, computers and the internet),UK
- Dictionary of criminal justice 7th Edition, California State University, Long Beach
- Kyalo Mbobu (2011) The law and practice of Evidence in Kenya lawAfrica publishing (K) Ltd
- Kiloba Richard (2011) Judicial Hints on civil Procedure 2nd Edition, lawAfrica publishing (K) Ltd
- Justice (Rtd) B.D.Chipeta(2010) Criminal law and procedure, A Digest of Cases, lawAfrica publishing (T) Ltd
- John W. Creswell and J. David Creswell (2017) Research design Qualitative and Quantitative and mixed methods approaches

*****