AGORA International Journal of Juridical Sciences, http://univagora.ro/jour/index.php/aijjs
ISSN 1843-570X, E-ISSN 2067-7677
Vol. 19, No. 1 (2025), pp. 71-86

A HUMAN RIGHTS PERSPECTIVE OF DIGITAL EVIDENCE IN SOUTH AFRICA

R. F. MAHMOUD

Rilwan F. Mahmoud
Faculty of Law, University of Ilorin, Nigeria
https://orcid.org/0000-0002-1162-149X, E-mail: mahmoudesq@yahoo.com

Abstract: *Recent border disputes and military hostilities have been at the centre of human rights violations accords the globe. A significant amount of evidence collected of the recent human rights violations tend to be digital and are stored electronically. This paper examines the rules regulating admissibility and weight of evidence in South Africa with a view to determining its adequacy in regulating electronically stored and generated information from such human rights violations. The article highlights the nature of digital information and the types of the medium with which they are displayed for the purpose of determining if evidence obtained from them can wholly be functionally equivalent to other classifications of evidence. The paper reveals that the current rules regulating electronic evidence in South Africa do not adequately accommodate electronically generated information and it recommends the enactment of an act exclusively regulating electronic evidence to prevent the miscarriage of justice.*

Keywords: *Electronic Evidence; Digitally stored Information*

1 Relevance of Electronic Information in Human Rights Violations

Following the recent Russian aggression against Ukraine, the 1991 Moscow Mechanism of the Human Dimension of the Organization for Security and Co-operation in Europe was triggered by Ukraine supported by 45 participating states in March 2022 (Office for Democratic Institutions and Human Rights ODIHR, 2022). The Moscow Mechanism stipulated that a team of experts conduct and complete a preliminary investigation into the alleged contravention of international humanitarian and human rights laws (ODIHR, 2022). A significant portion of the evidence obtained by the team of experts, showing 'clear patterns' of international human rights violations, where electronically stored information (ESI) in pictorial and video forms (ODIHR, 2022). Unfortunately, while electronic evidence has proven to be easily obtainable, verifying and authenticating electronic information has continued to pose a serious challenge. Evidence such as videos showing the alleged extrajudicial killings of civilians (men aged 16-60) in Bucha, a village in the Kyiv region, can serve as critical proof of crimes against humanity but only if its contents are adequately authenticated (Santa Monica Observer, 2022). There is, therefore, an urgent need to understand and determine the nature of ESI, particularly for the purpose of evidence in judicial proceedings (Mahmoud and Bellengere 2020).

Because of the ubiquitous nature of ESI, it often serves as the first piece of accessible information on social media platforms on human rights violations in recent years (Mahmoud

et. al., 2019). Electronic information in the form of videos, instant messages, pictures and text messages was beneficial in exposing and proving human rights violations in Africa, such as the killings of innocent civilians in response to the Boko Haram Insurgency in Nigeria (Walker, 2012). Due to the viability of evidence in the form of electronic information, there have been instances in which some countries restricts access to the internet and social media applications often for reasons of public safety and order (Kroff 2012). Between 2019 to 2020 alone, Benin, Gabon, Eretria, Malawi, Liberia, Mauritania, Tanzania, Ethiopia, Zimbabwe, Togo, Burundi, Chad, Mali, Guinea and Nigeria all restricted access to the Internet and social media applications (Giles and Mwai 2021). The restrictions in both Uganda and Tanzania occurred during the countries' election period while in other countries like Ethiopia and Nigeria, the internet restrictions often came after different forms of protests against the curtailing of human rights (Giles and Mwai 2021).

It is imperative to align the rules regulating evidence with the nature of electronic information with a view to improving the admissibility of, and weight to be ascribed to electronic evidence (Mahmoud, 2019). This paper examines the extant rules and procedures regulating evidence from electronically stored information in South Africa. While it will not delve into human rights laws, this paper evaluates the adequacy of the regulation of admissibility and weight ascription to ESI in the South African legal system.

2 Are the rules regulating ESIs in south Africa adequate?

The procedural rules regulating the admissibility of and weight to be ascribed to electronically stored information (ESI) in South Africa have been relatively unchanged and unquestioned for some time now, analysis of how electronic devices and their output fit into these rules has only recently begun (Tapper, 1974, Mason 2010, Collier, 2005). The diversity of these devices, their uses, and their complexity has only made it harder to apply evidentiary procedures to them (De Villiers,2010). They include the Civil Procedure Evidence Act (CPEA, 1965), Criminal Procedure Act (CPA, 1977), The Law of Evidence Amendment Act (EAA, 1988) and the Electronic Communications and Transactions Act (ECTA, 2002).

The conventional classifications of evidence in the South African legal system which include hearsay evidence, oral evidence, documentary evidence and real evidence, 'original and copy' and 'primary and secondary evidence' are some of the challenges that electronic evidence presents to conventional rules of evidence. The purpose of the ECTA is to facilitate the admissibility of data messaging as electronic evidence. Although the ECTA brought the much-needed legal recognition of data messages, it is submitted that it remains a challenging law with regards to the admissibility and weight of electronic information and its application has not been consistent. The court in *Jafta v Ezemvelo KZN Wildlife,(2008)* held that though the information contained in e-mail may contain informal language, evaluating such information as having no legal effect would be a mistake.

The ECTA sets out requirements for evaluating the weight of data messages which include the reliability and manner in which it was generated, stored or communicated and the manner in which the originator was identified and in which the message was maintained (Section 15, ECTA). It also sets out requirements for the admissibility of information contained in data messages that were created by a person in their ordinary course of business. It also introduces definitions including data which it defines as the 'electronic representation of

information in any form'(S1, ECTA). The act also defines data message as information created and stored on an electronic device in any format which includes animation, pictures, and sounds. Other relevant definitions include 'automated transaction', 'electronic communication', 'writing' (S12 ECTA) and 'signature'. (S13, ECTA) While the ECTA is no doubt a highly commendable piece of legislation as it recognised the abovementioned issues, it does have a few shortcomings, as discussed below.

One major point of contention that the ECTA has failed to resolve is the definition of a document with respect to data messages. The implication of this is Section 34 of the CPEA, 221 of the CPA and Section 3 of the EAA, among others, which applied to traditional paper documents still apply to electronic information and must be read together with the provisions of ECTA for the purpose of admissibility and weight to be ascribed thereto (*Narlis v South African Bank of Athens* 1976). The problem with this is that the application of these Sections to data messages might create absurdities because these Sections were not originally designed with electronic information in mind (Watney, 2009). Section 34 of the CPEA, for instance, provides for a statement made by a person in a document to be admissible. However, this is of little help as a computer is not regarded as a person.

The definition of a document, which includes any device by which information is recorded or stored, is wide enough to include a computer itself (S vs. Harper 1981). A document as defined by both the CPA and CPEA has been interpreted to include everything that contains written or pictorial proof of something regardless of what material it is made of. This definition has led to the opinion, by some scholars, that data messages fall conveniently within the realm of what constitutes documents (Watney, 2009). This opinion seems to be backed up by the apparent functional equivalency created by the ECTA which states that the criteria that information contained in a document must be in writing will have been fulfilled where such information was created in data form on an electronic device and is retrievable in a visibly intelligible form (S12 ECTA). This section seems to equate the rules of admissibility and weight of documents to those of a data message by rendering them of the same nature (Hoffman, 2010).

There is, therefore, a need for clarification of the definition and nature of what constitutes documents in relation to electronic information by way of an amendment or the enactment of an electronic information evidence act. Another matter to be considered is the lack of clarification of the difference between an original and a copy of electronic evidence in the ECTA (South African Law Reform Commission, (SALRC, 2010).

While the ECTA provides that courts should not deny the admissibility of data messages merely for the reason of not being in its original form, it does not provide the definition of 'original' or 'copy' of a data message (S11 ECTA). Section 14 of the ECTA states that the requirement of "originality" will be satisfied if the data message can be produced, in either electronic or paper format and that evaluation of the integrity of the content of a data message is a necessary requirement as well as the purpose for which it is being tendered into evidence. It is submitted that it is necessary to clearly differentiate between an original and a copy of a data message because unlike documents in paper form, a data message on an electronic device may be transferred through different storage media or software causing it to undergo changes (SALRC, 2010. A clear and concise test of originality would provide courts with a guarantee that the electronic information presented as output is the same as the

information that was generated on the device as input. Such an analysis usually focuses on the operational accuracy of the information system in recording, maintaining, transmitting and displaying the data message (Theophilopoulos, 2015).

Another inadequacy in the current system is the lack of clarification on whether Section 3 of the EAA applies to computer-generated evidence (Van De Merwe, 2016). The Law of Evidence Amendment Act (EAA) was introduced to provide rules regulating the admissibility of hearsay evidence. Even with the legal recognition as well as the assured admissibility of data messages by ECTA, (Sections 11 and 15) some scholars have opined that Section 3 of the EAA should also apply to electronic evidence (Van De Merwe, 2016). This position is predicated on the argument that although it is possible for the creation of a data message to require little or no direct human influence, all computer printouts occur with some form of human intervention because computer programmes are written by humans thereby making the probative value of the data message dependant on the credibility of someone who is not testifying (Collier, 2005). The need for drawing a difference between the real and documentary nature of data messages is because if a data message is adjudged to be real evidence then Section 3 of the EAA will obviously not apply to it as its evidential value is not predicated on another person (Schwikkard and Van der Merwe, 2016). The issue remains unsettled and therefore clarification is required as to whether a data message constitutes hearsay within the contemplation of Section 3 of the EAA and, if so, whether it applies to data messages made with little or no human effort Ndlovu v Minister of Correctional Services and Another (2006).

Another point of contention is the scope of Section 15(4) of the ECTA which appears rather broad and uncertain (Zeffertt et. al., 2003). The Section makes a data message in any form, be it a copy, printout or an extract, made by any person in the ordinary course of business, admissible as rebuttable proof upon certification by an officer in the service of the maker of the data message. In *Absa Bank Ltd v Le Roux (2014)*, the court was of the opinion that:

> Section 15(4) has a twofold effect. It creates a statutory exception to the hearsay rule and it gives rise to a rebuttable presumption in favour of the correctness of electronic data falling within the definition of the term ‘data message'.

Though the ECTA provisions regarding admissibility and weight are based on the UNCITRAL Model Law, Section 15(4) is an apparent departure from the Model Law (SALRC, 2010) and the Section runs the risk of opening a floodgate of data messages that now enjoy a presumption of genuineness on the mere production thereof (Collier, 2009). The law, therefore, needs to be reviewed with specific consideration given to the nature of electronic information.

3. Are ESI printouts inherently Real evidence or Documents?

Printouts of electronic data like any other piece of evidence are subject to the hurdles of admissibility and weight (Angus-Anderson, 2021). The real dilemma is in determining which hurdle best suits the nature of an electronic printout. Computer printouts on paper have for a long time been interpreted to fit into the ‘ordinary meaning of the word document’ (Harper, 1981, De Villiers,1993 and Ndiki, 2008). This position has proven to be far from settled as there continue to be many debates on whether printouts are exclusively documents or documents at all (Hoffman, 2010).

Writings on a piece of paper by a person constitute a document, however, when such a process passes through an electronic device it may not necessarily be so. All computer printouts occur with some form of human intervention because software itself is a set of human written codes and instructions (Collier, 2005). All electronic printouts are as a result of some form of programming and human instigation and even the simplest human-generated document is processed by the computer. Mason (Mason, 2010) puts it succinctly thus:

> Software is written as source code. The source code is written by the programmer, by entering instructions in an editor. The sequence of instructions defines the function of the program, such as taking input from the user, performing calculations, showing output on the screen and so on. This source code is then usually compiled into an executable program (an executable file causes a computer to perform tasks in accordance with the instructions), which is distributed to the users of the program. The source code cannot be derived completely from the executable program.

It is pertinent to note that documentary or real evidentiary qualifications are not inherent in a computer printout. Rather, what determines which evidentiary rules will apply is the purpose for which such evidence was produced. In determining the admissibility and weight to be ascribed to documentary evidence, the court will consider whether or not such evidence is the best evidence usually by examining its originality or the strength of its duplicate. The court may also consider its author in determining the truth of its content (Krige, 2012). In the case of real evidence, the court will mostly focus on different rules such as the reliability, functionality, and accuracy of the producing equipment in determining the reliability of the content of the real evidence (S vs. Ndiki 2008). Unlike documentary evidence, best evidence and originality rules do not ordinarily apply to real evidence *(HNP v Sekretaris van Binnelandse Sake* 1979).

4. The role of the Contents of ESI printouts in determining applicable evidentiary rules

The nature of the information contained on a printout from an electronic device determines whether rules of documentary or real evidence should be applied. Likewise, the process of generating printouts; with or without human intervention can also help determine whether the printout should be treated as a document or as real evidence (Law Commission, Report LCR, 1997). This form of classification has been recognised in one way or another by several eminent scholars (D T Zeffertt et. al., 2003, Tapper, 1974, Mason, 2010, Collier, 2005, Hofman, 2010 Van der Merwe, 2014 and Watney, 2009). For the purpose of this evaluation, the classification of computer printouts by Advocate Roux Krige shall be adopted. Krige's classifications of electronic printouts are most relevant to this research because they identify the differences between documentary evidence and real evidence that pose documentary traits (Krige, 2012). Krige's classification helps pinpoint the aspects of electronic information that may not fit into the traditional classifications of evidence; they are as follows (Krige, 2012).

1. The information in the printout came about as a result of the computer having processed raw data which was entered into the computer by a person.
2. The information was recorded by mechanical means without the personal involvement of a human being.

3. The information in the printout was entered into the computer by a person in circumstances where the computer did not process the information so entered.

4.1 Where the information in the printout came about as a result of the computer having processed data entered into the computer by a person.

An example of this classification of a printout can be found in the use of Microsoft Excel. Microsoft Excel is a computer application designed for the purpose of storing, organising, and manipulating electronic data fed into it by a person. The application uses numbers and text on spreadsheet styled electronic files and contains roughly a million rows and more than 16,000 columns. The programme is also designed to incorporate dates and times, Boolean values and formulas that enable it to draw inferences and make calculations based on the data imputed without human assistance. It is necessary to make a distinction between statements generated as a product of artificial intelligence and statements based on information supplied by a human being (LCR, 1997). This is because it is possible to produce data messages with little or no human intervention and this brings into question the extent to which such a data message can be termed documentary evidence (Hoffman 2010).

Also, the printout of information from an electronic device may not contain rooted information that is present in the electronic form *(Trend Finance (Pty) Ltd v Commissioner of SARS* 2005).

The printouts in this category contain statements that were not created by a person because the electronic device with its software calculates sorts, collates, and synthesises the entered data fed in by the user. It then gives it back in a different format to that in which it was entered into the computer (Krige, 2012). The weight ascribed to the information contained on such a printout depends on the functionality of the electronic device. Such a statement may be included in a document produced by the device as the printout but it could equally be displayed on the screen of the electronic device that created or even a voice output that can be played back in the format of an oral statement (LCR, 1997).

4.2 Where the information was recorded by mechanical means without the personal involvement of a human being.

Printouts in this category are those generated by devices and applications designed to function almost exclusively in isolation from human involvement. The role to be played by the user is usually limited to activation or confirmation. An example would be an automated teller machine (ATM). An ATM is a data terminal, with input and output interfaces, which connects to, and communicates through, a host processor. The processor is synonymous with an Internet service provider (ISP) in that it is the process by which ATM networks are displayable to the cardholder. Interactions with the ATM are performed by input devices which may include a card reader, keypad, scanner, and cash depositor and also output devices which may include a speaker display, screen receipt printer, and cash dispenser. Unlike recording/displaying functions on some electronic devices, the ATM merely receives instructions and executes the commands accordingly. This is often accomplished when the cardholder/user inserts their PIN into the keypad, which the ATM scrambles and transfers, alongside the information from the magnetic stripe, to the financial institution through a system network like MasterCard. This enables banks to examine the PIN imputed against the data on their records (Murdoch, 2009).

This will then prompt the ATM to carry out functions based on the instructions of the cardholder/user.

In this category, the electronic system is activated by a person without any other involvement. The electronic information is created by an algorithm that has been pre-encoded into the electronic system (Krige, 2012). This type of a printout falls into the class of real evidence because it consists of tangible evidence which does not include statements by a person that would have otherwise rendered them hearsay(Schwikkard and Van der Merwe, 2016). Unlike documentary evidence, the rules of hearsay evidence do not apply to real evidence (Bellengere, 2013). Real evidence does not rely on the testimony of any author. Rather, if any oral testimony based on real evidence is required or offered, it usually is with respect to matters of accuracy, reliability, and regularity.

In the case of *S v Ndiki and Others (2007),* the court reiterated that a data message that was created solely on the functionality of the electronic device and its internal software constituted real evidence. In *Ndiki's* case, the state tendered some computer printouts in proof of charges of fraud against the accused. The court held some of the computer printouts as being documents because their veracity depended upon the credibility of a signatory. The court held the other computer printouts to be real evidence because they did not require any such corroboration as they were made with little human intervention. The court, in interpreting Section 15 of ECTA, held that the section aimed to address information from data message as real evidence as contemplated by common law. This was also affirmed by the Supreme Court of Appeal in *Spring Forest Trading CC v Wilberry (Pty) Ltd t/a Ecowash (2015)* where it stated as follows:

> [The aim of the ECTA] is to promote legal certainty and confidence in respect of electronic communications and transactions, and when interpreting the Act, the courts are enjoined to recognise and accommodate electronic transactions and data messages in the application of any statutory law or the common law.

4.3 Where the information in the printout was entered by a person in circumstances where the computer did not process the information.

In this category, the data in issue is fed into the electronic device by a person. The data is then produced as a printout in the same format as it was entered into the device (Krige, 2012). Examples of this include writing an email, text message or drafting a document in Microsoft Word where printouts of these bear the exact content fed into the electronic device by a person. This form of a printout is regarded as a document and the truth of the statement contained therein is subject to the credibility of the author. In such a case, the probative value of the statements contained in the printouts will be determined by proving the truth of the facts contained therein (LCR, 1997).

However, there are complications where chats have been stored through a replication process that involves alteration by a third party. An example of this occurred in the United States in the case of *United States v Jackson (2007),* where the court decided that the information contained on a printout did not accurately capture the chat as it was on the electronic device, thus it was not an acceptable duplicate of the original version. Also, in the *Ndlovu* case (2006) the printouts in question were recorded entries of parole violations and

this was why the court treated them as documentary evidence and applied rules regulating documents in determining their admissibility and ascription value.

Furthermore, it is pertinent to determine the following question: at what point should electronic information contained on a printout be excluded? There are two potential answers to this; the first of which is that such a printout is hearsay (LCR, 1997). This is because the information contained in it as it can be likened to a statement made by a person who imputed it into the electronic device. The other view is that the truth of the statement contained in the printout is predicated on the accuracy of the information contained in it.

Therefore, if the accuracy of the data is proved, the statement contained therein is not capable of possessing probative value by its nature so the question of whether or not it constitutes hearsay becomes a non-starter because the statement itself is irrelevant. The United Kingdom Law Commission made this observation in a report on hearsay and recommended as follows:

> It is, therefore, unnecessary to complicate our hearsay rule by extending it to statements made by machines on the basis of human input. On the other hand, we do not think it would be safe to assume that everyone will share this view. We must anticipate the argument that, if such statements are inadmissible at present, that is because they are hearsay; that, under our recommendations, they would no longer be hearsay, because our formulation of the rule would apply only to representations made by people; and that they would, therefore, cease to be inadmissible... We recommend that, where a representation of any fact is made otherwise than by a person but depends for its accuracy on information supplied by a person, it should not be admissible as evidence of the fact unless it is proved that the information was accurate (LCR, 1997).

It is submitted that the consequence of this with respect to the South African law of evidence, is that the present evidentiary regime is not sufficiently flexible (Collier, 2005). This is because the transient nature of ESI makes its creation, transfer, and storage unique as compared to other forms of evidence like written documents or real evidence, therefore, the application of the conventional rules will the aforementioned instances, be inadequate.

5 The implication of 'Purpose' in determining the admissibility of, and ascription of value to, electronic information

The purpose for which evidence is sought to be tendered is essential in determining its evidential classification as well as the weight to be ascribed to it. The importance of purpose transcends the classification of the quality of evidence as either original or secondary and this is because sometimes the same document is primarily for one purpose and secondary for another (Malek et. al., 2005). This also applies to electronic data which is information that can be generated, processed or stored by electronic means. Data messages can contain a statement or several statements and can be tendered for multiple purposes (Theophilopoulos, 2015).

Determining the accuracy or inaccuracy of the data message is a different matter from determining the truth of the statement contained in the data message. The effect is that different admissibility and value ascription rules may apply depending on the purpose it is tendered. For example, a data message in the form of a video recording wherein ***Mr. A*** tells ***Mr. B*** that he was robbed at gunpoint might be tendered for the purpose of implying that ***Mr. A*** does, in fact,

know ***Mr. B.*** The data message will be admissible once it is shown to be an accurate representation of the information purported to be contained therein. The same data message might be inadmissible as hearsay if it is tendered for the purpose of proving the truth of the statement contained therein i.e. to prove that ***Mr. A*** was indeed robbed.

Another example can be drawn from the facts of *Offenback v L.M. Bowman, Inc. (2011)* (a matter in the United States) in which an action arose from a vehicle accident that occurred on 6 November 2008. The plaintiff claimed he suffered physical injuries to his right shoulder and lower back as well as psychological injuries which rendered him unable to drive for a period of time and which physically limited his riding of a bicycle or motorcycle. The court, in determining the relevancy of the plaintiff's posts detailing his trips between Kentucky, Virginia, and Pennsylvania, held as follows:

> [O]ur review of Plaintiff's Facebook account reveals the following potentially relevant information that should be produced to Defendants. Plaintiff has posted a number of photographs or updates that reflect he continues to ride motorcycles and may have on more than one occasion travelled via motorcycle between his home in Kentucky and Pennsylvania. In particular, our review found a photograph posted on March 14, 2011, which appears to show Plaintiff with a Harley Davidson motorcycle that other posts suggest that he purchased in or around July 2010. On or about October 1, 2010, Plaintiff posted information to his account that suggests he may have travelled to West Virginia via motorcycle. On July 22, 2010, a post on Plaintiff's "Profile" page suggests that he had taken, or was planning to take, a trip to Pennsylvania on his motorcycle...

The defendants did not intend to prove the truth of the contents of the photographs but intended to draw implied assertions from them which suggested that the plaintiffs' claims that he suffered physical and psychological injuries which rendered him unable to drive and limited his riding of a bicycle or motorcycle were bogus.

In other to determine what evidentiary rules ought to be applied to electronic information, the purpose for which it is being tendered is therefore of primary importance. Evidence containing statements has two primary purposes for which it might be tendered. Firstly, to establish the truth of its content and secondly to establish the fact that it was made so as to make implied assertions. This paper evaluates the impact of these classifications on the rules governing the admissibility and ascription value to electronic information as follows:

1. Electronic information tendered for the purpose of drawing implied assertions.
2. Electronic information tendered for the purpose of proving the truth of its content.

5.1 Electronic information tendered for The purpose of drawing Implied Assertions

An implied assertion is created where inferences are drawn from express facts in the content of evidence being tendered (LRC, 1997, *Caswell v Powell Duffryn Associated Collieries (1939) and S v Naik,* 1969). It is the inference of facts made possible by the existence of some assertions put forward as evidence in a statement such as a bystander saying to another person (in a United Kingdom matter), '[y]our place is burning and you going away from the

fire!' The court was duty bound to infer from the statement the defendant was at the scene which he had hitherto denied (Teper v. The Queen, 1952). The rationale behind these inferences from expressly asserted facts is that it is not always the case that the expressly asserted facts or statements are relevant or important to the case. Rather, the inferences might be a crucial determinant (LCR, 1997). For example, where a minor describes a place that she believed an assault occurred, the express assertion is the carpet's colour she made mention of while the inference to be drawn by the court by how accurate her description was, is that the girl is indeed familiar with the room. While implied assertion is applied in governing admissibility and the ascription of value to statements contained in documents, it is submitted that these rules can also be applied to electronic information as well. For example, when a computer printout of surveillance footage showing the accused exiting the home of his alleged murder victim is tendered in evidence, the express assertion is that the accused was at the home of the victim at about the time of the murder. However, the implied assertion to be drawn by the court is that the accused has been to the victim's home, which he denies (LCR, 1997).

It is pertinent to point out that when evidence is 'relevant because of an inference which the court is invited to draw from it, questions of the admissibility of implied assertions will arise' and if the evidence is in the form of electronic information then, rather than the rules of hearsay being used to prove its truth (and which might render it inadmissible), the test of the accuracy of the information should be what the court concerns itself with (LCR, 1997). In the United Kingdom, the rules that shall apply if such inferences are to be drawn from electronic information are set out in Section 69 of the Police and Criminal Evidence Act (PACE Act, 1986) which requires that before a piece of evidence can be accepted, it must be shown that the electronic device from which it was extracted was in proper functioning condition:

> The purpose of Section 69, therefore, is a relatively modest one. It does not require the prosecution to show that the statement is likely to be true. Whether it is likely to be true or not is a question of weight for the justices or jury. All that Section 69 requires as a condition of admissibility of a computer-generated statement is positive evidence that the computer has properly processed, stored and reproduced whatever information it has received. It is concerned with the way in which the computer has dealt with the information to generate the statement which is being tendered in evidence of a fact which it states (*Director of Public Prosecution v McKeown*, 1997).

The implied assertion rule is applicable in any situation whether it is information that falls under the exceptions of hearsay or information in the category of real evidence (LCR, 1997). In South Africa, while the ECTA provides that the rules of evidence must not be applied so as to deny the admissibility of a data message merely on the grounds of its nature, it does not provide a distinction between the admissibility of a data message tendered to prove the truth of its contents and one tendered merely for inferences to be drawn from it (S15 of ECTA, 2002). The courts have, however, made an attempt in interpreting Section 15 of the ECTA on the admissibility of a data messages as they relate to hearsay rules particularly under Section 3 of the EAA in *Ndlovu Ndlovu v Minister of Correctional Services and Another (2006)*. The *Ndlovu* case makes a distinction between where the probative value of the information contained in data messages depends on the credibility of a person and where it does not depend on a person. The court held that the hearsay rules will apply in the first instance because nothing

in Section 15 suggests otherwise. In the second instance (where probative value of a data message doesn't depend on the credibility of a person), the court held that Section 3 of the EAA (which applies to hearsay evidence) will not apply as it was not intended to, instead, such data message should be admitted and due evidential weight accorded thereto 'according to an assessment having regard to certain factors'. While this is highly commendable, what *Ndlovu's* case fell short of establishing is the status of data messages that contain assertions of a documentary nature where the purpose of tendering them was merely to draw inferences rather than prove the truth of their content.

The difficulty that the ECTA might have created is that data messages tendered to show the fact that they exist rather than to prove the truth of their contents might still be subject to the hearsay rules. This is especially because a statement contained in a data message is capable of having multiple purposes when tendered as evidence in a judicial proceeding.

The fact that a statement may be used for multiple purposes was established in *R v Rice* (1963) where both 'the accuracy of the content of the document and the implications to be drawn from it were subjects of contention'. The information in issue was the content of a printout of an airline ticket which had been used up (LCR, 1997). The court was faced with determining the admissibility of the content of the ticket on the grounds that the information constituted hearsay. The Appeal Court decided that the ticket itself fell under the classification of real evidence but the information contained on it was hearsay and that 'the document must not be treated as speaking its contents for what it might say could only be hearsay'. As hearsay, the information on the airline ticket could not be admitted in evidence if it is tendered for the purpose of proving that it was issued to a person bearing the name on the ticket but in this case, the jury was allowed to make an inference from the information contained on the ticket that it had indeed been utilised by a person with the name on the ticket.

Another aspect to consider in determining the extent of the application of implied assertion to electronic information is where the item of electronic information is not one that asserts anything at all. This ought to be considered via an implied assertion made from a statement in a document where the speaker did not assert anything at all, such as a statement that cannot be analysed as true or false for example, a question or a greeting. In the case of *Kearley,(1992)* the court held that there was indeed an implied assertion in the statement. For example, 'where a child says "Hello daddy", the child is not "asserting": "I am speaking to my father", but a listener will be able to infer that fact, and that may be a significant inference in the case' (LCR, 1997). It is submitted that an implied assertion that electronic information which does not assert anything (such as metadata in form of time and dates, email headers, musical notes), can also be the subject of an inferred assertion where such information is crucial to proving the existence or nonexistence of facts in the case.

5.2 Electronic information tendered for the purpose of proving the Truth of its Contents

Unlike evidence tendered for the purpose of drawing an implied assertion, evidence tendered to prove the truth of its contents if it contains a statement is subject to the rules of hearsay and its exceptions (S3 of the EAA). This is because in placing reliance on the truth of the content of a statement, the best evidence is the testimony of the author or an original perceiver of the statement, without which the evidence is inadmissible. This crucial

differentiation of the reason between establishing the plausibility of what has been asserted and establishing the fact that it was asserted was made in *Subramaniam v Public Prosecutor(1956)* where the appellant was charged with illegal possession of firearms, his defence was that he was under duress by 'Malayan terrorists'. The attempt by the appellant to enter evidence into the court in respect of what exactly the terrorists had said in their threats was rejected by the court. On appeal, the Privy Council 'advised that the conviction had to be quashed because the reported assertions were tendered as original evidence to explain the accused's state of mind' adding that the intention of the terrorist to either carry out the threat or not was irrelevant to the case (LCR,1997).

Applying this rule to electronic information, when a data message is tendered as evidence to establish the fact that information was sent, received or stored it cannot be excluded merely because of that reason nor can it constitutes hearsay (Watney, 2009). Where, however, a data message is used to show the truth of its contents it may be excluded as hearsay on the grounds that the reliability of its content has not been sufficiently established and not because of the volatility of the information technology with which it was created (Hoffman, 2010). It is thus necessary to take into account the difference between form and content of evidence which is the basis upon which a court excludes a document as hearsay.

An illustration of this can be seen in *MTN Service Provider (Pty) Limited v L A Consortium & Vending CC t/a LA Enterprises and Others (2011)* where the plaintiff tendered computer-generated evidence to prove the delivery of the network services which the defendants did not pay for. The defendants objected to the admissibility of the computer-generated evidence on the grounds that it amounted to hearsay. The court held the data messages generated from the computer system required the direct evidence of the head of the department to verify its correctness as he was responsible for the correct capturing of the information into the computer system. If the printouts were, for instance, tendered to show an ongoing contractual relationship between the parties rather than the truth of the content, the direct evidence of the head of the department might not have been necessary. It has been argued that for this purpose, a data message tendered for the purpose of proving the truth of its content should be treated in the same manner as a document tendered for the same purpose, therefore, requiring the direct testimony of the author or an original of the data message (Hoffman, 2010).

6 Conclusions

South African evidentiary rules do not yet reflect the uniqueness of data messages because as things stand, the provisions of the CPA and the CPEA on the admissibility and weight of documents still apply to electronic information. The CPA defines a document as including any medium upon which information is recorded and preserved (S221(5)) of the CPA). The CPA also defines documents in relation to entries in accounting records to include a 'recording or transcribed computer printout produced by any mechanical or electronic device and any device by means of which information is recorded or stored' (S236(6)). The CPEA also has extensive regulations of documents in Sections 33 through 38 which also apply to criminal proceedings. While the courts have been restricted to adopting these provisions to electronic information there remains the possibility of misappropriation of these rules (S v. Harper, 1981). It is, therefore, necessary for evidentiary rules to be designed exclusively for the different types of data messages as well as the several possible contents of each data

message. On a similar note, while it is highly commendable that the ECTA emphasises the legal force of a data message (Bellenger and Swales, 2016), to take into account that data messages might are not all generic and might contain information of a real nature, or statements that may or may not be made by humans or a combination of them. Consequently, just like documents have different considerations for their admissibility; data messages being even more unique ought not to have a blanket admissibility status (Theophilopoulos, 2015).

It is, therefore, necessary for a review of the laws regulating the evidentiary procedure in South Africa. The South African Law Reform Commission (SLRC) has addressed some of these issues through their issue and discussion papers and has made several essential recommendations on some of the issues plaguing admissibility and weight of electronic evidence (SLRC, 2014). Some of such recommendations include the differentiation between information created in the form of data solely by a person and data created without the aid of human intervention. It also suggested reforms in the bill to make practice directions on the evaluation of both types of information. The SLRC also recommends that the rules of evidence should do away with the conventional 'presumption of regularity' when dealing with mechanical devices rather, it suggests that a limited presumption should be applied especially in civil proceedings which place an evidential burden on the other party who did not object on notice. It also recommends the enactment of a subsidiary practice direction on obtaining and producing information from electronic devices so as to help legal practitioners streamline the process of tendering evidence in data form and to help judicial officers with the more technical aspects of producing electronic evidence in court to avoid unnecessary confusion.

Another recommendation by the SLRC is the defragmentation of the rules of admissibility of documentary evidence to avoid the "apparent inconsistency" caused by solely amending the rules that are currently in force, or via a repeal of those rules and introducing instead, a unified body of laws designed to regulate information in data form created on electronic devices. Finally, the SLRC recommends a proposed draft bill (Law of Evidence Bill) which reflects the recommendations in its discussion paper 131: The Review of Law of Evidence (Annexure A (Law of Evidence Bill). The bill also provides some necessary definitions of certain terms including 'document', 'copy' 'electronic document', 'electronic document system', 'hearsay evidence' and 'business records'.

It is pertinent to point out that the SLRC discussion paper confirms one of the primary questions of this research; that the current regulations governing admissibility and weight of evidence in South Africa are inadequate. However, its recommendations, particularly the defragmentation of the rules of documentary evidence, removal of the presumption of regularity from the consideration of admissibility of ESI, and the proposed definitions contained in the Law of Evidence Bill do not fully take into consideration the nature of ESI. While the Law of Evidence Bill proposes some definitions such as 'document', 'copy' 'electronic document', 'electronic document system', 'hearsay evidence', and 'business records', it is the determination of this research that these definitions do not adequately address the transiency of ESI and are simply an attempt to fit aspects of ESI into conventional classifications of evidence. This is because the definition of 'electronic documents' in the proposed Bill, does not differentiate between a statement contained in an electronic form and information that cannot logically be considered statements.

It is also necessary to point out that the recommended Law of Evidence Bill [B B2014] explicitly states that it does apply to 'any rule of law relating to the admissibility of evidence rather, it applies specifically to the 'rules relating to hearsay, authentication and best evidence in relation to certain types of documentary evidence'. The implication of this provision is that any ESI that do not fall into the classification of documentary evidence will not be regulated by this bill. The bill attempts to compensate for this by extending the definition of electronic documents to include 'evidence that is produced wholly or partly by a machine or technical processes. It is suggested that the 'apparent inconsistency' sought to be avoided by solely amending and repealing extant rules will still remain if all forms of ESI and forced into the classification of documentary evidence.

In conclusion, it is the determination of this research that the conventional rules of hearsay, real and documentary evidence cannot pragmatically be applied to all forms of ESI and it is suggested that the SLRC's recommendations do not adequately address the lacunae. Consequently, it is recommended that there are clearer definitions of what constitutes electronic information which are statements, electronic information that is contained in documents and electronic information that are created wholly by electronic algorithms and software. It is also recommended that the rules regulating each of these types of information on authentication, best evidence, relevance, admission, presumption, and weight ascription are defined individually to avoid inconsistencies in evidence classification.

REFERENCES

Articles

1. A Walker 'What is Boko Haram' (United State Institute of Peace, June 2012) www.usip.org/sites/default/files/resources/SR308.pdf (Accessed on 11th January 2022). Videos purportedly showing the extrajudicial execution of alleged Boko Haram members by the police, including a former commissioner in the state government were posted on YouTube.D Kroff 'Social Media and Human Rights Issue Discussion Paper' (Commissioner for Human Rights- Council of Europe, 2012) <rm.coe.int/16806da579> Accessed on 12th January 2022.
2. Adrian Bellengère & Lee Swales "Can Facebook ever be a substitute for the real thing? A Review of *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012" (2016) (5) SA 604 (KZD) *Stell LR* 454 at 466.
3. Bellengère A *et al The Law of Evidence in South Africa* (2013) Oxford University Press.
4. C Giles & P Mwai, 'Africa internet: Where and how are governments blocking it?' (BBC News, 14 January 2021) <www.usip.org/sites/default/files/resources/SR308.pdf> (Accessed on 12th January 2022).
5. Colin Tapper "Evidence from computers" 8 *Georgia Law Review* 562 1973-1974
6. D Collier "Evidently not so Simple" (2005) *The Quarterly Law Review for people in business* Vol 13(1) ISSN 1021-7061
7. D T Zeffertt, P Paizes, and A St Q Skeen, *The South African Law of Evidence* LexisNexis Butterworths Durban (2003) 393-395.
8. D Van der Merwe "A Comparative Overview of the (Sometimes Uneasy) relationship between digital information and certain legal fields in South Africa and Uganda" 2014 http://dx.doi.org/10.4314/pelj.v17i1.07 (accessed 20 June 2021)
9. D W Collier 'Electronic Evidence and Related Matters' in P J Schwikkard et al *Principles of Evidence* (2009) 3rd ed. Juta & Co Wetton 416-7.

10. De Villiers D S "Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 1)" (2010) *Tydskrifvir die Suid-AfrikaanseReg* at 558.
11. De Villiers D S "Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 2)" 2010 *Tydskrifvir die Suid-AfrikaanseReg* 720.
12. G. P. van Tonder "The admissibility and evidential weight of electronic evidence in South African legal proceedings: a comparative perspective" Being a thesis submitted in partial Fulfilment of the requirements for the LLM degree in the Faculty of Law of the University of the Western Cape. 2013 at 18.
13. Hofman J 'South Africa' in Mason S (ed) *Electronic Evidence* (2010)
14. M Watney "Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position" (2009) http://go.warwick.ac.uk/jilt/2009_1/watney (accessed on 5 June 2016)
15. Malek, HM (ed) *et al Phipson on Evidence*, Sixteenth Edition, Sweet & Maxwell, London (2005) 1192.
16. R Krige "The Admissibility of Electronically Generated Evidence in a court of law" a paper presented at the Cybercon Africa Convention Emperor's Palace Johannesburg 24-25th October 2012.
17. Rilwan F. Mahmoud & Bellengere, A. H 'A social service? A case for accomplishing substituted service via WhatsApp in South Africa.' (2020) 137(3) The South African Law Journal 371, 374-375.
18. Rilwan F. Mahmoud "The Potential of WhatsApp as a Medium of Substituted Service in the Nigerian Judicial System" (2019) Malaysia Current Law Journal, Legal Network Series. A (cx iii); 1.
19. Rilwan F. Mahmoud, Abdulazeez, H. O. & Wuraola, O. T. "An Assessment of the Legal Recognition and implementation of Electronic Evidence in the Tanzanian and Nigerian Legal Systems" (2019) The Public and International Law Journal, University of Abuja. 1(1).
20. S Mason *Electronic Evidence* (2010) 2nd ed (Lexis Nexis))
21. Santa Monica Observer, 'Russian Army Executes Hundreds of Civilian Men in Bucha, Other Kyiv Suburbs. Bodies Litter the Streets with Hands Tied Behind Backs' https://www.smobserved.com/story/2022/04/01/news/russian-army-shot-all-men-aged-16-to-60-in-bucha-7000-civilians-killed-if-true-biggest-warcrime-of-the-war/6642.html (Accessed on 1st April 2022).
22. Schwikkard P J & Van der Merwe S E *Principles of Evidence* 4th ed Juta Cape Town 2016 437 – 446
23. South African Law Reform Commission Report Review of the Law of Evidence "Electronic evidence in criminal and civil proceedings: admissibility and related issues" (Issue paper 27, Project 126) 2010 para 6.13.
24. Steven J Murdoch "Reliability of Chip and Pin evidence in banking disputes" (2009) *Digital Evidence & Elec. Signature* L. Rev. Vol 6 98.
25. Theophilopoulos C "The admissibility of data, data messages, and electronic documents at trial" (2015) *Tydskrifvir die Suid-AfrikaanseReg* 468.
26. Van der Merwe D *et al Information and Communications Technology* 2nd ed LexisNexis Durban 2016.
27. Wendy Angus-Anderson "Authenticity and Admissibility of social media website printouts" http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1282&context=dltr (accessed on 24 December 2021).

Judicial Decisions

28. *Caswell v Powell Duffryn Associated Collieries Ltd* 1939 All ER 722; *S v Naik* 1969 2 SA 231 (N).
29. *De Villiers* 1993 (1) SACR 574 (Nm)
30. *Director of Public Prosecution v McKeown* [1997) NLOR No. 135, (House of Lords).
31. *HNP v Sekretaris van Binnelandse Sake* 1979 (4) SA 274 (T).
32. *Jafta v Ezemvelo KZN Wildlife* (2008) ZALC 84.
33. *Kearley* [1992] 2 AC 228.
34. *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A).
35. *Ndlovu v Minister of Correctional Services and Another* [2006] 4 All SA 165(W) at 173.
36. *Offenback v L.M. Bowman, Inc.* 2011 West Law 2491371 (M.D. Pa. June 22, 2011).
37. *Rice* [1963] QB 857, 872
38. *S v Brown* 2016 (1) SACR 206 (WCC).
39. *S v Harper*1981 (2) SA 638 (D).
40. *S v Ndiki* 2008 (2) SACR 252 (Ck) 261d-h (para 54).
41. *Seccombe v Attorney-General* 2002 (2) All SA 185 (Ck) 277
42. *Spring Forest Trading CC v Wilberry (Pty) Ltd t/a Ecowash* 2015 (2) SA 118 (SCA).
43. *Subramaniam v Public Prosecutor* [1956] 1 WLR 965.
44. *Teper v The Queen* [1952] AC 480.
45. *Trend Finance (Pty) Ltd v Commissioner of SARS* (2005) 4 All SA 657 (C).
46. *United States v Jackson* 488 F. Supp. 2d 866, 869-70 (D. Neb. 2007).

Laws

47. Civil Proceedings Evidence Act 25 of 1965
48. Electronic Communications and Transactions Act 25 of 2002.
49. Law of Evidence Amendment Act 45 of 1988
50. Police and Criminal Evidence Act of 1986
51. The Criminal Procedure Act 51 of 1977

Reports

52. Law Commission, Report Law Com No 245 Evidence in Criminal Proceedings: Hearsay and Related Topics, 1997 Paragraphs 7.42-7.50.
53. Office for Democratic Institutions and Human Rights (ODIHR) "Report on violations of international humanitarian and human rights law, war crimes and crimes against humanity committed in Ukraine since 24th February 2022" (Being a report presented to the delegations of the OSCE participating states) ODIHR.GAL/26/22/Rev.1 13 April 2022.
54. South African Law Reform Commission "Discussion Paper: The Review of Law of Evidence" (Paper 131, Project 126, 2014) para 3.1.