PARTICIPANTS' PAPERS

ADMISSIBILITY OF DIGITAL/ELECTRONIC EVIDENCE IN MALAWI

*Golda Chilembwe Rapozo**

I. INTRODUCTION

Digital/electronic evidence comprises of evidence found on electronic devices and can be relied on in a court of law.[1] This evidence includes, videos, voice recordings, text messages and electronic transactions to name a few. With the advancement in technology, more crimes are being committed online. People now solicit or offer bribes through text messages or e-mails. Bribes are often received through electronic monetary transfers rather than through cash. This has triggered an increase in digital forms of evidence for the Anti-Corruption Bureau. However, in Malawi, digital evidence is still a novel concept and, thus, not largely adjudicated on. This paper will analyse the admissibility of digital evidence in Malawi.

II. STATUTORY PROVISIONS

The starting point with regard to evidence in Malawi is the Criminal Procedure and Evidence Code (CP & EC). The Criminal Procedure and Evidence Code is the guidebook regarding the treatment and admissibility of evidence as well as procedure in criminal proceedings. The general rule under the Criminal Procedure and Evidence Code is that all admissible evidence must be relevant.[2] However, this does not mean that all relevant evidence is admissible. It must further be noted that the Criminal Procedure and Evidence Code is an old piece of legislation that was enacted at a time when Malawi did not envision that there may be evidence that would be submitted electronically and, due to this, the Criminal Procedure and Evidence Code unfortunately does not provide for the treatment of digital evidence.

In 2016, the Electronic Transactions and Cyber Security Act was enacted in Malawi. One of the reasons for the enactment of the Act was to provide for investigation, collection, and use of electronic evidence.[3] The Act makes a distinction between electronic messages and electronic records. Section 3 of the Act defines electronic messages as any communication created, sent, received or stored by electronic communication means, such as computerized data exchange systems, electronic mail systems and instant messaging. Examples of electronic messages may include e-mails, WhatsApp Messages and voice notes sent between parties. The most important qualifier is that electronic messages are about communication between individuals. Electronic records on the other hand are defined by the same section 3 of the Act as any record created, generated, sent, communicated, received and maintained by electronic means. This includes videos, pictures, documents and audio that are recorded for the sole purpose of recording and not to be used as communication.

Sections 15 and 16 of the Act provide for the authentication and admissibility of electronic evidence. Section 15 provides that the originality of an electronic record will be satisfied if:

(a) There is reliable assurance of the integrity of the electronic record;

(b) The electronic record is capable of being displayed to the person to whom it is to be presented.

* Senior Legal and Prosecutions Office, Legal and Prosecutions, Anti-Corruption Bureau, Malawi.
[1] https://nij.ojp.gov/digital-evidence-and-forensics
[2] Sections 171 and 172 of the Criminal procedure and Evidence Code.
[3] Short title of the Electronic Transactions and Cyber Security Act.

The criteria for assessing the integrity of information is stated to be: whether it has remained complete and unaltered, save from the addition of any endorsement and any change which may arise in the normal course of communication, storage and display. As for the standard regarding admissibility of electronic evidence, the Court will consider:

(a) The reliability of the manner the electronic record was generated, displayed, stored or communicated.

(b) The reliability of the manner in which the integrity of the information was maintained and stored.

(c) The manner in which the originator of the electronic evidence was identified and any other factor that the Court may deem relevant.

III. JUDICIAL PRECEDENT

The courts in Malawi will generally view electronic evidence, including videos, voice recordings and text messages as hearsay evidence and, thus, not admissible. In the case of *Brown Mpinganjira v Dumbo Lemani and Davis Kapito*,[4] the court stated that a video recording is not admissible in court as it is considered hearsay evidence unless there is testimony defining and describing the provenance and history of the recording up to the moment of its production in court. This was a contempt of court case where the plaintiff was accusing the defendants of uttering defamatory statements about him in the media even though the court had ordered that the case was not to be discussed in the media. As proof of the defamatory remarks, the plaintiff brought a video tape which showed the defendants uttering the disparaging remarks at a political rally. The court, however, refused to admit the video recording as evidence, arguing that mechanically produced evidence is susceptible to tampering and unless its authenticity and chain of custody is established, the Court would be remiss to admit it as evidence and doing so would be putting the court in danger of infringing the constitutional rights of the defendants.

This decision was followed in the case of *Dr. Thomson Mpinganjira v The Republic*.[5] This was a bail hearing pending the determination of an appeal. The substantive case involved an attempted bribery of constitutional court judges in the 2020 elections case in Malawi. The principal witness in the case was a judge who recorded phone calls between himself and the accused person where the accused person was asking for a phone number of the chairperson of the constitutional court case, claiming that he had a package to deliver. The evidence was tendered by the judge who recorded the phone calls, and the accused person admitted that it was indeed him on the other end of the line. The court at first instance deemed the recordings admissible and the accused was convicted of attempted bribery. However, the appellant is now seeking an appeal and in the application for bail pending appeal, the convict argued that his case had a high likelihood of success seeing as how the evidence that convicted him should not have been admissible in the first place.

The court agreed that the case had a high likelihood of success upon appeal because, following the decision in the *Brown Mpinganjira* case, the audio recording should not have been admissible. The court stated that:

> *The Human Rights and Freedoms enshrined in our Constitution will be rendered useless if the trial courts are not cautious and do not get satisfied or do not warn themselves of the danger of audio recordings as well as about the source and history of this type of real evidence. It should not matter that the Appellant confirmed or admitted a conversation ensued between him and a prosecution's witness. If such were to happen, would it not mean that the courts of justice will be allowed to admit illegally obtained evidence like for example wiretapping without the sanction of the court? It is trusted that the Court will investigate these questions on appeal if they arise. In any event, it is common knowledge that accused's evidence should never be used to augment the evidence of the prosecution.*

[4] Civil Cause No. 222 of 2001.
[5] MSCA Criminal Appeal No. 9 of 2021.

IV. CHALLENGES

Having looked at the legal framework with regard to the admissibility of electronic evidence in Malawi, it is important to note that the implementation of the law is not without issues. Firstly, considering the fact that in order for electronic evidence to be admissible, it must be authenticated, and a proper chain of custody must be established, there are issues of expert witnesses that would need to be paraded in order to establish the same. This brings on issues of lack of structures and personnel that can properly extract and preserve the evidence from the electronic devices without tampering with the authenticity of the evidence.

In order to curb this, the government and state agencies must invest in training investigators in digital forensics and state-of-the-art digital forensic labs, thus ensuring that issues of admissibility due to authenticity and chain of custody are of no consequence.

Another aspect that needs to be considered when admitting electronic evidence is the source. Most of the time, electronic evidence is evidence gathered after a seizure or as a result of phone tapping. There has been an argument in the courts that evidence obtained through search, seizures and phone tapping is illegally obtained evidence as it violates the accused person's right to privacy. However, the courts have dealt with this matter by stating that whether to admit such illegally obtained evidence is at the discretion of the court. In the case of *Mike Appel & Gatto Limited v Chilima*,[6] the court stated that:

> *Where evidence is obtained illegally, improperly or unfairly, two opposing views exist, one in favour of admitting the evidence as long as it is relevant and necessary, and the other view is to exclude it regardless of its relevance and whether it is necessary. The former position represents English common law while the latter represents the view that rejects the fruit of the poisonous tree in some jurisdictions. Malawi has over time followed the English common law position that a court will exercise discretion to admit relevant evidence if in its view the probative value outweighs the prejudicial effect. That remains the position under Malawi law.*

This was also echoed in the recent decision in the case of *The state on the Application of Kezzie Msukwa & another v The Director of the Anti-Corruption Bureau*,[7] where the Court held that:

> *There is no rule of law in Malawi to the effect that illegally obtained evidence is inadmissible as Counsel sought to suggest. It is my conclusion that the position in Malawi mirrors very closely that which was articulated by the Supreme Court of Ghana, which is that save for instances where the law as prescribed expressly disallows evidence obtained in specific circumstances amounting to violation of certain rights guaranteed by the Constitution or other law, the framework of our constitution and indeed our broader legal system anticipates that where evidence obtained in violation of human rights is sought to be tendered in proceedings, whether criminal or civil, and objection is taken, the court has to exercise its discretion and decide on a case by case basis, whether on the facts of the case, the evidence ought to be excluded or admitted.*

This is an ongoing case in which the evidence that led to the arrest of the accused persons was obtained through phone tapping. The accused persons brought a judicial review matter questioning the constitutionality of the arrest considering that the evidence was illegally obtained. This decision has propelled the fight against corruption in Malawi considering the fact that corruption is never conducted in the limelight. It has thus been hard for the Anti-Corruption Bureau in particular to balance the gathering of relevant, admissible evidence and the suspect's right to privacy.

[6] MSCA Appeal No. 30 of 2014.
[7] Judicial Review Cause No. 54 of 2021.

V. CONCLUSION

The handling of electronic evidence before the courts in Malawi is still in its infancy. There has not been a lot of jurisprudence regarding the issue of admissibility of electronic evidence, and Malawi still struggles from lack of technological advancement. Despite all this, all parties – including investigators, prosecutors and the courts – will have to adjust their perspective as the world is changing quickly and crime and the evidence proving the crime is no longer what it was. All parties involved in the justice system should focus on learning from other jurisdictions which have made advancements in the way they handle electronic evidence, which will, in turn, improve the way we handle corruption cases in Malawi.