ADMISSIBILITY OF COMPUTER EVIDENCE UNDER SRI LANKAN CRIMINAL PROCEEDINGS : A COMPARATIVE ANALYSIS

HMMC Herath

Faculty of Law, General Sir John Kotelawala Defence University, Sri Lanka
mayomiherath@gamail.com

Abstract - Sri Lanka has now stepped into a new global era having overcome the terrorism which resulted in a rapid technological advancement.. This study seeks to answer the problem present legal regime pertaining to computer evidence provide appropriate mechanisms to ensure the admissibility of computer evidence in Sri Lankan criminal courts and if the findings to that question is in the negative, what reforms should be brought upon to strengthen the law regime on this respect. The primary objective of the study is to examine the existing legal framework on computer evidence currently entertained in criminal proceedings in Sri Lanka with certain other jurisdictions. The secondary objective is to identify the loopholes of the present legal framework and to propose apt recommendations to reform the existing legal regime on the admissibility of computer evidence in Sri Lanka. The research was executed using two methodological approaches. The black letter approach was utilized for a profound analysis on the legal provisions pertaining computer evidence. Empirical research methodology was used to gather information on the current status of the computer evidence and its practical implication. Ultimately, this study raises certain pertinent questions in the legal framework on computer evidence still remain unanswered. The main focus of the study revolves around the significant provisions of the Evidence (Special Provisions) Act of 1995, the Evidence Ordinance of 1895(As amended by Act No 29 of 2005) and the Electronic Transactions Act of 2006.

Keywords - Admissibility, Computer Evidence, Criminal Proceedings, Sri Lanka

I.INTRODUCTION

Evidence in the sphere of law, is said to be intrinsic in character: for it includes the material objects or statements which could be submitted to a competent court in determining the accuracy of any claimed matter of fact under investigation. Hence, Law of Evidence is incidental to heterogeneous challenges with the global technological evolution, especially with the invention of computers. The main concern of this paper is on the current laws applicable in Sri Lanka regarding the admissibility of computer evidence under criminal proceedings along with its position with the cognitive laws of the US and England. The research problem seeks to answer whether existing provisions in the statues relating to the computer evidence, safeguard mechanisms to ensure that electronic evidence will be admissible under criminal proceedings in Sri Lanka and what measures are necessary to be introduced, in order to ameliorate the admissibility in that regard.

II. METHODOLOGY AND EXPERIMENTAL DESIGN

Primary data of this research were acquired through semi-structured interviews with stakeholders in the Information Technology and Criminal Law regime such as lawyers, judges and expertise in the respective fields .Secondary data was gathered via the content analysis method where the researcherdeducted and analysed data from various materials such as books, journals, newspaper articles, websites which were related to the admissibility of computer evidence in Sri Lanka.

III. APPLICABLE LAWS AND RESULTS

1. Evidence Ordinance of 1895

Section 3,the interpretation clause, of the Evidence Ordinance has curtailed the term ”evidence” to include

oral and documentary evidence, hence it has been enabled by certain provisions of the Evidence Ordinance, to produce substantial objects as evidence when the circumstances require. Nevertheless our courts have admitted contemporaneous recordings of public speeches, telephone conversations through wire or tape recorders and photographs as evidence, despite of the exclusion of real evidence in Section 3 of the Ordinance. In the case of, The King v Dharmasena (1950) 51 NLR 481, Canakeratne, J. has expressing his views, on the value of photographic evidence stated that "may be the cameras do lie in terms of long focus lens and not holding at eye-level, hence one wouldn't provide with all the witnesses since there are perjurers. If real evidence could be brought to the court and if a jury can view a scene, why not a photograph?"

2. Evidence Special Provisions Act of 1995 (ESPA 1995)

Courts were disinclined to admit documents generated by the computer as evidence, prior to the enactment of the ESPA 1995. This skeptical attitude of the courts can be observed in Benwel v Republic of Sri Lanka (1978-79) Sri. LR 194, where Colin Thorm J. declared that "Computer evidence is neither original nor derivative, it is in a unique category. In order to accept such documents, the court must satisfy that they have not been subjected to any alteration. None of the sections in the Sri Lankan Evidence Ordinance make reference to computer evidence…". However, a hindsight was given in terms of computer evidence with the technological development occurred in computer transactions. ESPA 1995 was drafted as a consequence of this reconsideration.

It is noteworthy that under ESPA 1995 what is admissible is a "statement produced by a computer". In the absence of the said phrase a question occurs as to the determination of the scope of admissibility. It is suggested that evidence are of two kinds; computer generated evidence and computer stored evidence. The amalgamation of the above two categories may also constitute evidence. However at present there are no judicial or scholarly regulations in Sri Lanka to provide guidance as to the exact scope of admissibility. Furthermore, in the UK, R v. Blackburn (and Wade) [2005] All ER (D) 392 (May), addressing the issue of when is a document produced by a computer, the court was reluctant to accept a word processed document as a document produced by a computer.

Section 4 of the ESPA 1995 now enables a party to a dispute to confer any contemporaneous, electronically made, audio or video recording or reproduction as evidence. Although the term "computer" has defined to include any device which stores and process information, ESPA 1995 does not define the term "electronic". It is noteworthy that under this provision purely mechanical recordings can be produced as evidence. Only an electronical or mechanical recording or reproduction can be tendered as evidence under Section 4(1) (a), that is to say the recording must be supported by oral evidence in terms of relevancy. Such evidence may consist of a person who truly heard the conversation. Supreme Court observed in the case of K.H.M.H. Karunaratne v. The Queen (1966) 69 NLR 10 "the trial judge should have assessed the experts' evidence before considering the tape record in proving the risk in attempting to identify the speakers by their voices in tape recorders the greater risk of such identification in tapped telephone conversation.

It is vital to note that the device used to make a recording or reproduction was functioning properly. In the UK case of R v. Spiby[1991] Crim.LR 192, it was held that although computer-generated evidence does not contain human errors, but the real evidence does. This decision was overruled with the recognition of the computer error. Subsequently in R v. Cochrane(C.S.) (CA) 15 June 1992,established for the first time that computer evidence should explain the nature and the function of the computer system, before ascertaining the application of Section 69(1) of the Police and Criminal Evidence Act of 1984. Non alteration of the recording or reproduction during or after making it, keeping it in custody is another requirement. Thus practical and theoretical issues have resulted due to the effortless alteration.

It is important to assess whether the provisions of ESPA 1995 is in conflict with the concept of hearsay rule; which generally means that evidence in all cases must be direct. The case of Somasiri v. The Queen (1969) 75 NLR 172, includes application of the hearsay rule. This was a murder case where the prosecution led testimony of two witnesses who claimed that the deceased, few days before her death informed his father about a warning on the accused visiting the house. The court held, referring to Section 60 that the testimony of the two witnesses are inadmissible by the reason of them being hearsay and not direct. The appropriate witness in such an event would be the father of the deceased. One has to determine whether the evidence is hearsay or not depending on the purpose it has been led. Consequently if a computer record is to be considered as evidence, the witness should be the person who entered the details to the system as he is the only one who aware on

the input. Moreover, hearsay rule could not be applied to all computer records such as automatic records which are kept without human intervention.

The principle of rule against hearsay is entitled to express statutory recognition in countries like the US and the UK although it is not firmly incorporated into Sri Lankan law. For an instance the Federal Rules of Evidence, in its US Rule 801(c) interprets hearsay as "a statement, excluding one formed by the declarant, while claiming at the trial, produced as testimony to prove the veracity of the matter asserted". The hearsay rule was applied in the Iowa State, the US in State v. Colwell 715 N.W.2d 768 (Iowa Court of Appeals, 2006), which involved a cybercrime, where Colwell appealed against his two counts which amounted making of a false report under a statue of Iowa. The Iowa court established that "since the lacuna of a human declarant required by the rules of evidence, the computer generated records tracing calls between certain phone-numbers which this case include are not hearsay".

The rationalization of the rule against hearsay to such electronic records retained by computers without any human intervention was brought forward by the Supreme Court of Louisiana in The State v. Armstead432 So.2d 837 (Louisiana Supreme Court 1983). The court expressed its views stating that neither the printout itself nor the printout of the computer's integral operation results are hearsay evidence as it does not include the output of the statements put into the computer by court declarants. Such statements are generated without an oath so that their accuracy cannot be assessed by cross-examination. As per a machine, inaccurate data will only generate if such machine is not operating properly.

In the UK, Section 114 of the Criminal Justice Act 2003 defines hearsay as "a statement except an oral evidence given by a person in the proceedings, which is submitted as evidence on the stated matter". By the reason of certain computer records produced before the court constituted hearsay, House of Lords had very reluctantly acquitted an accused in Myres v. Director of Public Prosecutions[1965] AC 1001 (HL). Although following this case a reconsideration of the law of hearsay evidence brought forward by strong judicial calls, no alterations were made until the Criminal Justice Act 1988, which enabled acceptable records made during business, an exemption to the rule of hearsay.

The position in both the US and the UK is that hearsay rule is not attracted by automatic recordings of information. Thus in R v. Dodson Williams [1984] 1 WLR 971 (CA), a security camera which was in operation during a robbery was accepted as evidence and the reasoning was that no application could be made to the hearsay rule, regarding the evidence created by a machine which automatically recorded an event. A witnesses who had seen the CCTV footage of an event was allowed by the court to give evidence on what they saw before the CCTV footage was accidently erased before the date of trial in Taylor v Chief constable of Cheshire[1987] 1 All ER 225 case. Court held that their evidence was direct evidence as if they've observed the scene through binoculars.

Section 6 and 7 of the ESPA 1995 lay down the process to be followed in rendering the computer evidence. As per Section 6 a party setting forth evidence permissible under section 4 or 5 is required to submit an affidavit made by a person of a responsible position regarding the function of the relevant machine, so as the requirement under section 4 or 5 is satisfied. Section 7 declares that before forty days of the trial or inquiry the party tendering evidence under Section 4 or 5 shall submit a notice to the opposite party including a list of evidence along with a copy of such evidence, adequate to enable the party to understand the nature of such evidence. A party receiving such notice may within fifteen days from the receipt of such notice apply the party giving the notice to inspect the evidence ought to be provided, the device which produced the evidence, or any records on that regard. It is noteworthy that the procedure regarding electronic evidence under the ESPA 1995 is different that of in the Criminal Procedure Code of Sri Lanka.

3. Electronic Transactions Act of 2006 (ETA 2006)

ETA 2006 was introduced to identify and expedite the establishment of contracts, the initiation and exchange of data messages, electronic documents, electronic records, and other electronically formed communications. ETA 2006 is to be applied not in conflict with the Evidence Ordinance or any other written law. If any information included in a data message, electronic document, electronic record or other communication made by a deceased or by reason of his physical or mental condition is unfit to attend as a witness or is outside Sri Lanka and where reasonable steps have been taken to find such person and he cannot be found or who fears to give oral evidence or who is prevented from so giving evidence, evidence regarding such information shall be accepted.

Certain presumptions are enacted by ETA 2006 by its Section 21(3). As regard the first presumption, it is of the candidness of the data message, electronic document or electronic record. This is a dramatic reversal of well-known hearsay rule. Emerging of any data message, electronic document or record from the person who claims to have made it would be the second presumption. Thirdly, the genuineness of any electronic signature will be presumed by the court. It is an obvious fact that these presumptions could be rebutted by proving the contrary. ESPA 1995 in contrary, confines its presumptions only to include the truthfulness of any contemporaneous recording or statement furnished by a device or a computer of common use. Nevertheless, it is proposed that such generalized devices may lead to unauthorized tampering which may cause uncertainty.

The Courts shall, unless proved in contrary, postulate the truth of information contained in a data message, electronic document, electronic record or other communication and in respect of a person who made any data message, electronic document, electronic record or other communication, that it was made by the person who is claimed to have made it and shall surmise the genuineness of any electronic signature or distinctive identification mark.45 A delicate approach has been taken by the legislature to accept electronic evidence and the burden of proof of the genuineness of such document has been effectively moved from proposing party to the opposing party.

Marine Star (Pvt.) Ltd v. Amanda Foods Lanka (Pvt.) LtdH.C. (181/2007(MR) decided on 31.07.2008, involved an issue regarding the admissibility of a text message (SMS) where Chithrasiri J. observed that SMS is a document that is to say as per the definition given for the term "document" in the Evidence Ordinance which includes data stored on hard disks or other form of permanent or temporary storage devices. In addition SMS is also acceptable under Section 21(2) of the ETA 2006 since it was sent during the course of business.

As per the UK, the Electronic Communications Act 2000 made the UK one of the first countries to effectively legalize e-signatures in the world.On the other hand, the Electronic Communications Privacy Act 1986 of the US has categorized levels of privacy protection, depending on how important or sensitive the information is.

4. Payment Devices Frauds Act of 2006

Section 16 of the PDFA 2006 is concerned with the matters regarding evidence under the same Act. Correspondently, a certified copy of an entry relating to a payment device inside or outside Sri Lanka, kept by an Issuer or acquirer in his ordinary course of business, whether in writing or way of by electronic, magnetic, optical or any other methods, in an information system, computer or payment device shall be accepted as evidence relation to a prosecution as for an misdemeanour under section 3 of the Act, and shall be prima facie evidence of the facts stated.

IV. DISCUSSION AND CONCLUSION

The ESPA 1995 has facilitated the acceptation of computer evidence by removing obstacles such as the rule against hearsay, which previously prevented the admission of such evidence. Regarding to contemporaneous recordings created by electronic or mechanical methods by a machine or a properly operating device, the most critical issue is whether the recording was altered or modified so as to affect its authenticity and reliability. The evidence of forensic experts might become important in dealing with this issue. Relating to computer evidence, it is important to ascertain whether the information provided to the computer was accurate. Here again the evidence of data entry operators who put information into the computer becomes important characters. The ESPA 1995 focuses on the admissibility and not on discovery of computer evidence. As per criminal investigation, there does not appear to be any issue regarding the seizure, examination and production in court, of any device or computer used in any criminal offence. The field of forensically sound computer evidence has been evolved to receive and investigate information contained in computers and other devices, which has become vital evidence in a criminal matter. The enactment of legislation such as the ESPA 1995 may not by itself be adequate to deal with issues arising in technological development which constituted computer evidence. It is also essential to improve the required skills among investigators, computer forensic experts, lawyers and judges to tackle the issues arising from computer evidence and to provide the necessary equipment and infrastructure for the courts to confront with the challenges of this new field of evidence.

Issues arise in pragmatism where there are contradictions in the provisions of ESPA 1995 and ETA 2006. There is no applicability of the ESPA 1995 in relation to any data message, electronic document, electronic record or other

document to which the provisions of ETA 2006 applies. Another important issue need to be resolved is the express exemption of the applicability of the ESPA 1995 in Section 22 of the ETA 2006, rendering the change brought by the Evidence (Amendment) Act 2005 as nugatory.

To summarize, the law of evidence relating to computer records and statements in Sri Lanka has developed over the years. In terms of the economic development, it is necessary to embolden electronic transactions and remold Sri Lanka into a paperless environment. Computer forensic investigators must be aware of the legal environment in which they work, or they risk of having the evidence obtained being ruled as inadmissible. Nevertheless it is important for the public to have confidence in the legal system and its ability to incorporate types of electronic evidence in order to make use of the technological development and to ensure personal and commercial safety. Even though many positive changes has commenced in respect of the admissibility of computer evidence under criminal proceedings, in terms of the ESPA 1995 and the ETA 2006, the law is currently confronted by ambiguity which requires to be elucidated imperatively.

References

Abeyaratne, S., 2008. Introduction to Information and Communication Technology Law. 1 ed. s.l.:Sunil D.B Abeyaratne.

Alwis, M. P. L. D., 2018. PC, LLB (Colombo), LLM (Colombo), Lecturer [Interview] (13 May 2018).

Amarawickrama, S., 2008. The Development of the Law of Evidence in Sri Lanka into the 21st Century. Bar Association Law Journal, Volume 1, p. 175.
Anon., 2006. Island.lk. [Online]
Available at: www.island.lk/2006/11/08/midweek4.html
[Accessed 09 May 2018].
Marsoof. S., Computer Evidence In Criminal And Civil Proceedings n.d. Lawnet. [Online]
Available at: <https://www.lawnet.gov.lk/1960/12/31/electronic-computer-evidence-in-criminal-and-civil-proceedings/
[Accessed 09 May 2018].

Bainbridge, I., 2000. Introduction to Computer Law. 4 ed. s.l.:Pearson Education Ltd.
Dharmasena, K. v., n.d. [Online]
Available at: https://www.lawnet.gov.lk/1977/12/31/the-king-v-dharmasena/
[Accessed 09 May 2018].

Electronic Communications Act 2000

Electronic Communications Privacy Act 1986

Electronic Transactions Act 2006

Evidence (Amendment) Act 2009

Evidence Ordinance 1895

Evidence (Special Provisions) 1995

Fernando, J., 2005. Electronic Transactions Legislation; Background and Features. Bar Association Law Journal, Volume 11, p. 82.

Kevan, T. a. M. P., 2010. E-mail, the Internet and the Law. 1 ed. s.l.:Universal Law Publishing Law Co. Pvt. Ltd.
Lanka, B. v. R. o. S., n.d. Lawnet. [Online]
Available at: https://www.lawnet.gov.lk/1979/12/31/benwell-v-republic-of-sri-lanka/
[Accessed 09 May 2018].

Lloyd, I., 2011. Information Technology Law. 6 ed. s.l.:Oxford University Press.

Marsoof, S., 2006. Electronic Transactions in the Modern World. Sri Lanka Law College Law Review, Volume 4.

Marsoof, S., 2009. Electronic and Computer Evidence in proceedings before Courts and Labour Tribunals. Sri Lanka Bar Association Law Journal, p. 9.

Mason, S., 2012. Electronic Evidence. 2 ed. s.l.:LexisNexis Butterworths.

Murphy, P., 2000. Murphy on Evidence. 5 ed. s.l.:Universal Law Publishing Law Co. Pvt. Ltd.
Queen, K. v. T., n.d. Lawnet. [Online]
Available at: https://www.lawnet.gov.lk/1977/12/31/k-h-m-h-karunaratne-appellant-and-the-queen-respondent/
[Accessed 05 May 2018].

Queen, S. v. t., n.d. Lawnet. [Online]
Available at: https://www.lawnet.gov.lk/1977/12/31/d-somasiri-appellant-and-the-queen-respondent/
[Accessed 09 May 2018].

Sampson, G., 2009. Law for Computing Students. 6 ed. s.l.:Geoffrey Sampson & Ventus Publishing ApS.

Soyza, S., 2008. Electronic Evidence in Sri Lanka. Sri Lanka Bar Association Law Journal, Volume 14, p. 204.

Stephan, M. a. S. D., 2017. Electronic Evidence. 4 ed. London: Institute of Advanced Legal Studies, University of London.

Talagala, D. C. S., 2018. LLB(Hons), LLM(Hons), PhD(Griffith), Consultant, Visiting Lecturer [Interview] (13 May 2018).