KDU Law Journal
General Sir John Kotelawala Defence University, Sri Lanka

Volume 02, Issue 01
March, 2022

ISSN 2783-8870

Admissibility of Computer Evidence in Sri Lankan Courts: A Comparative Analysis with Other Jurisdictions

Shalini Fernando*

Abstract

The information technology is one of the constantly evolving and emerging subjects in the global arena. Gathering, conservation, communication and presentation of the computer derived evidence must fulfill legal requirements with regard to the admissibility of computer evidence. Computer evidence that was gathered in a way that was not in accordance with the law will be declared inadmissible. In many jurisdictions there was a challenge in admissibility of computer evidence. Evidence (Special Provisions) Act, No. 14 of 1995 and Electronic Transaction Act, No. 19 of 2006 two special legislations enacted for the admissibility of computer evidence in court proceedings in Sri Lanka.

In considering the current situation in Sri Lankan justice system, there is a dual regime governing admissibility of computer evidence and it has resulted number of issues in terms of admissibility of computer evidence. Further Sri Lankan judiciary in several cases, has taken up two different approaches while interpreting the prevailing law of admissibility of computer evidence. Therefore, there is an uncertainty in Sri Lankan system relating to admissibility of computer evidence. Therefore, it is high time to find a comprehensive solution to resolve this lacuna in Sri Lankan law.

Keywords: *Admissibility, Admissible evidence, Computer Evidence, Judicial discretion, Legislation, Legal System*

* LLB (Hons) (Jaffna), LLM (Colombo), Diploma in Forensic Medicine and Science (Colombo), Attorney at Law

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

Current Legal Framework Governing the Admissibility of Computer Evidence in Sri Lankan Courts

According to the No 14 of 1895 of the Evidence Ordinance of Sri Lanka there are two types of evidence namely oral evidence and documentary evidence[1]. However, there is no universal or unique interpretation for the Computer evidence. In terms of the provisions of the guidelines and explanatory memorandum on Electronic Evidence in Civil and Administrative Proceedings issued by the Council of Europe, "Electronic Evidence (Computer Evidence) is defined to mean any evidence derived from data contained in or produced by any device, the functioning of which depends on a software programme or data stored on or transmitted over a computer system or network[2]".

Neither Sri Lankan Evidence (Special Provisions) Act nor the Electronic Transaction Act No:19 of 2006 does not interpret "Computer Evidence". However, in the light of several interpretations made on the computer evidence[3], Computer Evidence can be defined as, any evidence that created, recorded, stored, or produced or transmitted in electronic form and includes computer evidence, digital audio and video, mobile phones, digital fax machines and any evidence that is derived from electronic devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras and other portable equipment such as data storage devices and the internet and it can be created from digital devices such as telecommunication or electronic devices.

When considering the statutory provisions in Sri Lanka, there are no provisions in the Evidence Ordinance of Sri Lanka in respect of the admissibility of computer evidence. In terms of the section 03 of the Civil Law Ordinance No:05 of 1852 as amended, "*in all questions or issues which may hereafter arise or which may have to be decided in Sri Lanka with respect to the law of partnerships, corporations, banks,*

[1] Section 03 of the Evidence Ordinance of Sri Lanka.
[2] Guidelines and Explanatory Memorandum on Electronic Evidence in Civil and Administrative Proceedings adopted by the Committee of Ministers of the Council of Europe on 30th January 2019.
[3] Guidelines and Explanatory Memorandum on Electronic Evidence in Civil and Administrative Proceedings adopted by the Committee of Ministers of the Council of Europe on 30th January 2019.

and banking, principals, and agents, carries by land, life and fire insurance, the law to be administrated shall be the same as would be administrated in England in the like case, at the corresponding period, if such question or issue had arisen or had to be decided in England, unless in any case other provision is or shall be made by any enactment now in force in Sri Lanka[4]". However, Sri Lankan Judiciary has been very reluctant to apply this provision in judicial decisions.

Since there is no specific provision in the Evidence Ordinance with regard to admissibility of Computer Evidence, Sri Lankan legislature had to incorporate specific provisions into certain enactments in order to enable recognition of computer evidence. Intellectual Property Act, No.36 of 2003, Payment and Devices Act, No.30 of 2006, Computer Crimes Act, No.24 of 2007, Information and Communication Technology Act, No.27 of 2003, Payment and Settlement System Act, No.28 of 2005, are examples of such laws. In addition, to above legislations, the Evidence (Special Provisions) Act, No.14 of 1995 and Electronic Transactions Act, No.19 of 2006 (as amended) by Act No.25 of 2017 are two special statutes enacted for the purpose of admissibility of computer related evidence in court proceedings in Sri Lanka. These statutes have created a dual regime governing admissibility of computer evidence in Sri Lanka.

Moreover, it can explain a dual regime governing computer evidence in Sri Lanka as the Sri Lankan Judiciary in several cases has taken up two different approaches while interpreting the prevailing law of admissibility of computer evidence in Sri Lanka. However, it is a question whether the existing law is adequate to provide effective solutions to modern day challenges triggered by technological development and issues arising out of usage of computers and other devices. There is an uncertainty in Sri Lankan system when interpreting the existing law relating to the admissibility of computer evidence.

Commercial world has made several attempts to resolve issues relating to Computer Evidence. As a result in 1996, United Nations Commission on International Trade Law in its resolution adopted by the General

[4] Civil Law Ordinance No. 05 of 1982 section 03.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

Assembly adopted the Model Law on Electronic Commerce, which is well known as UNCITRAL Model Law on Electronic Commerce. UNCITRAL Model Law on Electronic Commerce (1996) mainly focused on the issue of legal obstacles in usage of electronic commerce.

In the year 2005, the United Nations Convention on the Use of Electronic Communications in International Contracts was adopted for the purpose of introducing globally recognized standards in the area of electronic commerce and to guide member countries in enacting their domestic laws. Especially as a result of the adoption of the ECC, developing countries in the South Asian region such as; Sri Lanka, India took steps to enact a special legislation in respect of the Electronic Transactions. Accordingly, in the year 2006, Sri Lankan legislature enacted the Electronic Transactions Act No:19 of 2006 as amended by Act No:25 of 2017.

In terms of the provisions of section 22 of the Electronic Transaction Act, nothing contained in the Evidence (Special Provisions) Act No:14 of 1995 shall apply to and in relation to ant data message, electronic document, electronic record or other document to which the provisions of this act applies[5]. Accordingly it is important to note that the provisions of the Evidence (Special Provisions) Act will cease to apply, when a given matter is within the domain of the Electronic Transaction Act.

In the light of the key provisions of the Evidence (Special Provisions) Act and the Electronic Transaction Act[6], it is very clear that there are separate provisions governing admissibility of computer evidence in Sri Lanka. And also there are separate requirements in both legislations in respect of admissibility of computer evidence in Sri Lanka. Furthermore, the Electronic Transaction Act has specifically excluded some important transaction from the Act. Moreover, a unique procedure is to be followed when placing evidence before the court. Therefore, it is obvious that when considering the aforesaid provisions of the Evidence (Special Provisions) Act No:14 of 1995 and the Electronic Transaction Act No:17 of 2006 as

[5] Section 22 of the Electronic Transaction Act.
[6] Section 3, 21 of the Electronic Transactions Act.

amended by Act No:25 of 2017, there is a dual regime governing computer evidence in Sri Lanka.

Judicial Approach of Sri Lanka in Respect of the Dual Regime Governed by the Evidence (Special Provisions) Act and the Electronic Transaction Act

As a result of the aforesaid dual regime governing admissibility of Computer Evidence in Sri Lanka, a number of issues concerning admissibility of computer evidence have come into light in recent time. When examining the several judgments delivered by the Sri Lankan judiciary in this regard, it can see emerging case law take two directions as describe below.

Prior to the enactment of the Evidence (Special Provisions) Act, the Sri Lankan judiciary was of the view that the computer evidence could not be admissible in terms of the Evidence Ordinance of Sri Lanka.

In ***Banwell v Republic***[7] Justice Colin Thome held that the computer evidence is in a category of its own. It is neither original evidence nor derivative evidence. Under the law of Sri Lanka, computer evidence is not admissible under section 34 of the Evidence Ordinance or under any other section of the Evidence Ordinance. In the case of ***P.C. Mayappan and Others v K.S. Manchanayake***[8] Justice Sansoni held that the mere stamping of the firm's name was not a sufficient signature within the meaning of section 92 (1) of the Bills of Exchange Ordinance for the purpose of rendering the firm liable as indorses[9].

However, in some decided cases the Sri Lankan Judiciary took up a different view in respect of admissibility of computer evidence prior to the enactment of Evidence (Special Provisions) Act. As an example it was held in ***M.S. Aby Bakr v Queen***[10] that *"the speech that is alleged to have been reproduced in Wijesena's hearing by means of the wire recorder is a fact that, in connection with the other facts alleged by the prosecution witness regarding the making of a speech by the appellant*

[7] *Benwell v Republic* (1978/79) 2 Sri L R 194.
[8] *P.C. Meyappan and Others v K.S. Manchanayake* 61 NLR 529.
[9] Ibid.
[10] *M.S. Abu Bakr v Queen* 54 NLR 566.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

and the recording and the reproduction of it, makes it highly probable that the appellant made a speech in the same terms on the occasion in question. Therefore, it is not a fact that is otherwise relevant, it is relevant under section 11 of the Evidence Ordinance[11]". In *in Re S.A. Wickramasinghe*[12] *Justice Gunasekara held that "The words imputed to him in the rule are quoted from a report which of his speech made on a "Grundig" tape recorder. Further it appears from the affidavits of four of the deponents, who say that they heard the speech that they heard the Respondent say about the judiciary what is imputed to him in this report. There can be no doubt that he did utter the words in question in a speech made at a public meeting held on the Galle Esplanade as alleged in the Rule*[13]". In ***Kularathne and another v Rajapakshe***[14] it was decided that a taped recording a statement made in a public speech could be admissible as evidence.

In the light of the aforementioned judgments, it is very clear that, prior to the enactment of the Evidence (Special Provisions) Act, the Sri Lankan judiciary was of the view that contemporaneous recordings of public speeches could be admissible as evidence[15]. Justice T.S. Fernando held that *"the admission of evidence of a wire recorded speech is not repugnant to our law of evidence. But the court should have considered the evidence of an expert who stated at the trial that (1) there are dangers in attempting to identify speakers by their voices as relayed through tape recorders and (2) the dangers attendant upon such identification are grater in a case where what is relayed is a telephone conversation*." In ***Shaul Hameed and another v Ranasinghe and others***[16] photographs marked in the Petition of a Fundamental Rights application showing the incident were admitted as evidence.

Therefore, it is important to note that in some cases prior to the enactment of the Evidence (Special Provisions) Act as well as the Electronic Transaction Act, some computer evidence were considered

[11] Ibid, 568.
[12] ***In re Wickramasinghe*** 55 NLR 511.
[13] ***In re Wickramasinghe*** 55 NLR 511, 512.
[14] ***Kularathna and another v Ranasinghe and Others*** (1990) 1 Sri L R 128.
[15] ***K.H.M.H.Karunarathne v Queen*** 69 NLR 10.
[16] ***Shaul Hameed and another v Ranasinghe and others***(1990) 1Sri LR 128.

as admissible evidence. However, there was no specific law and was no procedure to be adopted to adduce the computer evidence under the purview of the evidence ordinance of Sri Lanka.

After the Evidence (Special Provisions) Act and the Electronic Transaction Act came into the operation, the opinion in respect of the admissibility of computer evidence has changed. In the landmark judgment of ***Marine Star Pvt Ltd v Amanda Foods Lanka Pvt Ltd***[17] the then High Court Judge Chitrasiri held that "the message received on the screen of a mobile phone which had been typed by another person from a different point and was sent with the assistance of the technology could be admitted in evidence under and in terms of the section 21 of the Electronic Transaction Act, No.19 of 2006[18]". Therefore, it was opined that a short message received by a mobile phone in the instant case could be admissible as evidence under and in terms of the section 21 of the Electronic Transaction Act. In ***Millennium Information Technology Limited v DPJ Holdings (Private) Limited***[19] the Commercial High Court of Colombo has decided that printouts of a webpage can be adduced as evidence in Sri Lanka under the provisions of Electronic Transaction Act and it is not necessary to fulfill the procedure laid down in section 07 and 08 of the Evidence (Special Provisions) Act[20].

In the light of the said quotation of the order, it is apparent that the Sri Lankan courts were of the view that legal requisites stipulated in Evidence (Special Provisions) Act need not be adhered to in matters regulated by Electronic Transaction Act.

As per the decision of the ***Gallage Prabath Pieris v Jacquelin Isabella Aponsu***[21] the High Court of Civil Appeal of Western Province case it is obvious that the Sri Lankan courts have taken the stance that the Electronic Transaction Act does not apply to (personal transactions) and the party who is seeking to lead that type of evidence should follow the

[17] *Marine Star Pvt Ltd v Amanda Foods Lanka Pvt Ltd Case HC* (Civil) 181/2007 (MR) dated 31.07.2008
[18] At pages 5 and 6 of the Order.
[19] *Millennium Information Technology Limited v DPJ Holdings (Private) Limited HC* (Civil) 257/2009 MR.
[20] Ibid, 5.
[21] *Gallage Prabath Pieris v Jacquline Isabella Aponso*, WPHCCA(Col)156/2012 dated 11.07.2014.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

procedure laid down in the Evidence (Special Provisions) Act, and not the procedure set out in the Electronic Transaction Act.

In ***Chakrawarthige Vijitha Wijerathne v Munasinghelage Pathum Chamikara Sanjeewa and Hewakotambage Yamuna Chandrika***[22] a similar decision was reached by the court in a rent and ejectment matter. In ***People's Leasing Company LTD v Muthuthantrige Iran Fernando***[23] case held that; "*The Electronic Transaction Act defines the basic rule that no data messages, electronic document, electronic record or other communication shall be denied legal recognition, effect, validity, or enforceability, on the ground that it is in electronic form. (vide section 3 of the Act). Accordingly, I am of the view that such business Ledger (e.g., Accounts Ledger) is an electronic record within the meaning of section 26 of the Electronic Transaction Act No: 19 of 2006*[24]". Furthermore, it was clearly held in the judgment that in terms of the section 22 of the Electronic Transaction Act, Evidence (Special Provisions) Act No:14 of 1995 shall not apply to and in relation to any data message or any electronic document, electronic record, or other document to which the provisions of the Electronic Transaction Act apply.

In ***Commissioner General of Inland Revenue v Janashakthi Insurance Co. LTD***[25] the Court of Appeal decided that Section 3 of the Electronic Transaction Act is clear and there is no doubt that it has been put in place by legislature to facilitate the admission of the category of Electronic evidence. In the said judgment, Justice Surasena held; thus, "*This Court notes that section 3 of the Electronic Transaction Act has provided that 'no data messages, electronic document, electronic record, or other communication shall be denied legal recognition, effect, validity, or enforceability on the ground that it is in electronic form. There cannot be any room to doubt that the above provision has been put in place by the legislature to facilitate the admission of*

[22] ***Chackrawarthige Wijitha Wijerathne v Munasinghalge Pethum Chamikara Sanjeewa and Hewakotambage Yamuna Chandrika*** 2012 WPHCCA (COL) 44/2014/LA.
[23] ***People's Leasing Company LTD v Muthuthantrige Iran Fernando*** HC(CIVIL)201/2008 MR
[24] Ibid, 6.
[25] ***Commissioner General of Inland Revenue v Janashakthi Insurance Co. LTD*** CA (Tax) Appeal 10/2013.

the category of evidence referred to in the said section. Therefore, this Court has no hesitation to conclude that the provisions of law brought in by the Electronic Transaction Act No:19 of 2006, are procedural law provisions relating to evidence rather than any substantive law provisions relating to the regime of fiscal legislation[26]".

Furthermore, in a recent case, ***Independent Television Network v Godakanda Herbal Private Ltd and another***[27] Justice Eva Wanasundara held that under section 22 of the Electronic Transaction Act, No:19 of 2006 transcript of a statement of accounts can be admissible. In the said judgment the Supreme Court of Sri Lanka was of the view that the Electronic Transaction Act No:19 of 2006 was enacted specifically to promote technological advancement to be reckoned by the regime and section 22 of the said Act makes special provisions with regard to any data message, electronic document, electronic record or other document. Therefore, the computer generated running account and the summary of the same account can be admissible as evidence under the purview of the Electronic Transaction Act No:19 of 2006.

According to the legal principles laid down in the aforementioned judgments and orders of the judiciary of Sri Lanka, it is very clear that there are two directions have created in respect of admissibility of computer evidence in Sri Lankan Courts. And also there is no unique procedure to be adopted in Sri Lanka when considering and admitting the computer evidence. Therefore as mentioned earlier the unique procedure has to be followed when admitting the computer evidence. It is very important to note that these concerns need to be addressed in order to find suitable and effective solutions.

Analysis of the Sri Lankan System With International Guidelines and the United Kingdom and Singapore Jurisdictions

On the 30th January 2019, the Council of Europe adopted guidelines in respect of the Electronic Evidence in Civil and Administrative Proceedings. For the purpose of adopting the said guidelines the European Union

[26] Vide at page 23 of the Judgment.
[27] *Independence Television Network v Godakanda Herbal Private Limited and Others*. S.C.CHC Appeal 29/11.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

appointed a committee consists of the Ministers of the Member States and it was named as European Committee on Legal Co-operation.

In this respect, the guidelines are intended to strengthen the efficiency and quality of the justice[28]. According to the preamble of the guidelines, the said guidelines are applied only insofar as they do not contradict national legislation and that they are a non-binding instrument. Furthermore, it was aimed to ensure that specific challenges relating to electronic evidence are addressed, such as the potential probative value of metadata; the ease with which electronic evidence can be manipulated, distorted or erased; and the involvement of a third party (including trust service providers) in the collection and seizure of electronic evidence. Further it was stated in the guidelines that the said guidelines apply to the resolution of disputes in both civil and administrative proceedings.

Article 2 of the guidelines speaks about the way oral evidence is to be adduced via remote link[29]. As per Article 3 of the guidelines, it is the duty of the court to ensure that the procedure followed to take evidence is fair and effective[30]. In terms of the Article 4 of the guidelines, the procedure and the technologies applied to take evidence from a remote location should not compromise the admissibility of such evidence and the ability of the court to establish the identity of the person concerned[31]. Article 6 of the guidelines provides that courts should not refuse electronic evidence and should not deny its legal effect only because it is collected and/or submitted in an electronic form. Further in terms of the provisions of Article 7 of the guidelines in principle the court should not deny the legal effect of electronic evidence only because it lacks an advanced, qualified or similarly secured electronic signature. As per Article 8, courts should be aware of the probative value of metadata and of the potential consequences of not using it. Article 9 provides that the parties should be permitted

[28] Explanatory memorandum of Guidelines on Electronic Evidence Civil and Administrative Proceedings of Council of Europe Article 3.
[29] Article 2 of the guidelines.
[30] Article 3 (a) and 3 (b) of the guidelines.
[31] Article 4 of the guidelines.

to submit electronic evidence in its original electronic format, without the need to supply printouts. According to the aforesaid provisions 6 to 9 of the guidelines, it is important to note that the duty to ensure the originality of the computer evidence, and to ensure the legal effect of the computer generated evidence lie with the court.

As per Articles 10, 11, 12, 13, 14, 15 and 16 of the guidelines, the member states should establish procedures for the secure service and the collection of electronic evidence. In the light of the said provisions, data integrity, survivability, and security should be taken in to consideration when transmitting evidence.

Furthermore, Articles 17 and 18 of the guidelines speak about the relevancy of the computer evidence. According to these guidelines, it is the duty of the court to manage actively about the relevancy of the data and the necessity of the electronic evidence in the respective courts. Further, all electronic evidence should be considered on its merits.

Article 19, 20 and 21 of the guidelines speak about reliability of the computer evidence. Courts should consider all relevant factors concerning the source and authenticity of the electronic evidence[32].

Articles 22, 23 and 24 of the guidelines contain provisions regarding the integrity of electronic data[33]. In terms of Article 28 of the guidelines the courts should archive electronic evidence in accordance with national laws.

According to the aforementioned guidelines the member states have enacted relevant laws and have incorporated the guidelines into existing laws to give recognition to electronic evidence.

It is essential to note that in terms of the aforesaid guidelines set out in the Articles to the Explanatory Memorandum to the guidelines, it is evident that the European Union has always given recognition to the electronic evidence and aforesaid principles have been introduced in order to ensure

[32] Article 19 of the guidelines.
[33] Article 26 of the guidelines.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

the right to fair trial and the validity of admitting electronic evidence in a reasonable and justifiable manner.

However, when considering the Sri Lankan system, there is no such clear procedure in respect of evaluation and admission of the electronic evidence. The Sri Lankan system does not contain a procedure clearly addressing the relevancy, reliability and the authenticity of the computer evidence. Further, statutory Sri Lankan law including Evidence (Special Provisions) Act, and Electronic Transaction Act, lacks clear guidelines to evaluate the relevancy, reliability and the authenticity of the electronic evidence. Therefore, there is no proper mechanism in Sri Lanka to store and preserve computer generated evidence and to archive the data.

Law Relating to Admissibility of Computer Evidence in United Kingdom

When considering the jurisdiction of United Kingdom, there are three main legislations in operation governing admissibility of computer evidence. These statutes are Civil Evidence Act 1995, Police and Criminal Evidence Act 1982 and Computer Misuse Act 1992[34].

According to the Section 69 (1) of the Police and Criminal Evidence Act reads thus; "In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown; (a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;(b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to effect the production of the document or the accuracy of its contents[35]".

According to the aforesaid provisions of law in United Kingdom, it is evident that in criminal cases there is a strong legislative framework to facilitate the adducing of computer generated evidence. Comparatively, in Sri Lanka the existing law does not provide a unique procedure to be adopted for submission of computer evidence in criminal trials other than

[34] Guidelines issued by the UK Association of Chief Police Officers and the US National Institute of Justice.
[35] Section 69(1) of the Police Criminal and Evidence Act.

the procedure established in the Evidence (Special Provisions) Act, No. 14 of 1995, and the party who seeks to lead computer evidence must follow the procedure establish under section 7 of the Evidence (Special Provisions) Act.

Section 03 of the Computer Misuse Act 1990, basically covers the unauthorized access (hacking), unauthorized access to computer materials with intention to commit a further crime planting a virus, unauthorized modification of data such as deleting data, introduction of malware and spyware. It is argued that that courts in the United Kingdom encountered legal uncertainty regarding application made under section 5 of the Civil Evidence Act and under section 69(1) of the Police Criminal and Evidence Act. Especially it is argued in UK that the computer evidence are hearsay evidence or real evidence. In ***R v Spiby***[36] the Court of Appeal of UK held that printouts from an automatic telephone call logging computer installed in a hotel were admissible as they constituted real evidence.

In ***Castle v Cross***[37] the court decided that a print out from a device, or recorded on a mechanical measuring device can be considered as real evidence and it can be admitted. In ***Director of Public Prosecution v McKeown***[38] the House of Lords accepted the evidence in the information provided by an intoximeter although the computer clock was inaccurate. The court was of the view that the inaccuracy did not affect the processing of the information supplied to the computer.

Furthermore in ***Grant v South Western and County Properties***[39] the Supreme Court of United Kingdom has decided that a tape recording would fall within the ambit of the meaning and the interpretation of the term 'document'. In the said judgment the court of the view that the furnishing of information had been treated as one of the main functions of a document and the tape recording was accordingly a document.
In the light of the aforesaid judicial decisions the judiciary of the United

[36] *Comden London Borough Council v Hobson* [1991] Crim.L. R 199 (C.A. Cr. D).
[37] *Castle v Cross* [1984] 1 WLR 1372.
[38] *Director of Public Prosecution v McKeown* [1997] NLOR No.135, (House of Lords).
[39] *Grant v South Western and County Properties Ltd,* [1975] Ch 185, 2 All ER, 1975.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

Kingdom has always tried to interpret the existing law relating to Computer Evidence, in consist with the day today development of the technology and the computer related activities.

Law Relating to Admissibility of Evidence in Singapore

The fundamental source of the law of evidence in Singapore is the Evidence Act. This Act is not an exhaustive piece of legislation. In January 1989, the Government of the Singapore established a 'Trade Net' system and it introduced an Electronic Data Interchange (EDI) system for the purpose of offering solution for the issues arisen with development of the information technology. In order to find solutions to the issues, the Government of Singapore took steps to amend the existing Evidence Act and as a result the Evidence (Amendment) Act came into operation on 18th January 1996. Furthermore, in the year 1997 it introduced an electronic filing system to the judicial system to manage matters related to computer evidence.

According to the section 36(2) (e) of the Singapore Evidence Act, the court can call further evidence by affidavit given by an independent expert appointed or accepted by the court. Further the court may, if thinks fit, call for oral evidence of the deponent of an affidavit and or other issuer of the certificate concerning the accuracy of the computer output[40] Under the provisions of the section 35 of the Act, guidelines were provided on the weight of the evidence to be attached to any computer output tendered as evidence[41]. The court must consider all the circumstances from which inference can be reasonably drawn as to the accuracy, or otherwise or the computer output[42].

The Singapore court is given a wide and broad statutory power as well as the discretion in order to decide the accuracy of computer evidence adducing before court. However, when considering the Sri Lankan legislations, there are no such provisions to make use of when deciding on the accuracy of the computer evidence tendered before the court.

Further by introducing an amendment to section 65 of the Singapore

[40] Evidence Section 36(3).
[41] Evidence Act section 35.
[42] Evidence Act section 36(4).

Evidence Act, they have ensured that the admissibility of certain computer output as secondary evidence where the conditions for the use of such evidence is justified, where the original document has been destroyed[43].

Even though the aforesaid legal provisions of the Singapore Evidence Act reasonably address the legal issues in admissibility of computer evidence, the Singapore government has enacted a special law to govern e-commerce transactions called Electronic Transaction Act.

In the recent Judgment of ***Super Group Ltd v Mysore Nagaraja Kartik***[44] an email was admitted as the evidence under the provisions of the Evidence Act. In ***Alliance Management SA v Pendleton Lane P and Another***[45] the High Court of Singapore decided that producing of a computer printout, without producing of the original hard disk is admitted as secondary evidence under the provisions of section 35(1)(a) of the Evidence Act of Singapore.

Considering the totality of the facts set out in this chapter, it can say that United Kingdom and Singapore have several key legal provisions governing acceptance and admission of computer evidence in court proceedings, and that legal provisions of those countries are more comprehensive and adequate to address the issue of admissibility of computer evidence in trials. In contrast, there is a significant lacuna in the legal system in Sri Lanka in respect of adducing of computer related evidence in courts.

Recommendations and Suggestions

The proposal set out in this topic is for the development of the law and the procedure concerning admissibility of Computer Evidence in the Sri Lankan Courts.

Firstly, it can suggest introducing a unique and separate legislation addressing the issue of admissibility of Computer Evidence, (Digital Evidence, Electronic Evidence.) in all types of litigation in Sri Lanka. And

[43] Evidence Act Section 65 (c).
[44] *Super Group Ltd v Mysore Nagaraja Kartik* [2018] SGHC 192.
[45] *Alliance Management SA v Pendleton Lane P and Another* [2008] SGHC 76.

Volume 02, Issue 01
March, 2022
ISSN 2783-8870

also it has to introduce a special guideline and a special tool for the collection of computer evidence.

Secondly, it is essential to introduce a separate institution to support courts to identify the relevant computer related technical issues when considering computer evidence in court procedure.

Thirdly, it is suggested that it is highly important to conduct awareness programmes for Judges, Lawyers, Police Officers, as well as the public, on the importance of computer related evidence.

Fourthly, I suggest to introduce a suitable archiving service system in order to protect the validity of the data and to secure electronic evidence.

Conclusion

Admissibility of Computer Evidence is a critical issue in Sri Lankan since the legal system of the country creates a dual regime when admitting such evidence. The Evidence (Special Provisions) Act and the Electronic Transaction Act have created the said dual regime in the country. The Sri Lankan judiciary has opted to follow both these regimes.

There is no unique law in relation to the admissibility of computer generated evidence in Sri Lankan courts and there is no specific, standard guideline to follow in considering and placing computer evidence in Sri Lankan courts. Absence of a proper mechanism and a unique law, the judiciary has applied both these legal regimes in determining the admissibility of computer evidence.

Given the high number of computer related legal issues encountered by the judicial system, it is essential to have unique laws to adequately cover both substantive and procedural legal aspects concerning the admissibility of computer evidence in Sri Lanka. Moreover, there should be a clear and unique guideline to be followed in this regard by the relevant legal paternities of the country. Therefore, it is high time to find a comprehensive solution to resolve this lacuna in the Sri Lankan law.