AUTHENTICITY OF DIGITAL EVIDENCE AND CURRENT CHALLENGES

*Avantha Lakmal Bandara Wickramasooriya**

I. INTRODUCTION

There are 11.34 million internet users, 8.20 million social media users and 32.29 million mobile connections in Sri Lanka.[1] There were 3566 cybersecurity-related incidents reported in Sri Lanka in 2019, whereas, in 2022, 16,376 incidents were reported to SLCERT.[2] The cybercrime unit of the Sri Lanka Police department receives about 2,500 cybercrime incidents per year.[3] This speaks volumes of the amount of electronic evidence which the courts of Sri Lanka will encounter in the future. Irrespective of the nature of the crimes the final expectation of criminal trials is the acceptance of the electronic evidence presented in a case and proof of the guilt of perpetrators. The conclusion of the judge is based on the context or evidence he/she is satisfied with and understands. However, the law may establish certain evidential rules for the judge to adhere to.

The traditional Sri Lankan legal regime consists of the Penal Code, Code of Criminal Procedure Act, and The Evidence Ordinance. The advancement of the legal regime of Sri Lanka on information Technology commenced with Information and Communication Technology Act No. 27 of 2003. Thereafter, Intellectual Property Act No. 36 of 2003 was enacted with several new features in relation to the protection of software, trade secrets and integrated circuits in relation to the protection of intellectual property rights. To facilitate and govern the use of ICT in government and establishment of e-government services, the Electronic Transactions Act No. 19 of 2006 was enacted. This was based on the standards established by the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996) and Model Law on Electronic Signatures (2001). The Payment and Settlement Systems Act No. 28 of 2005 and Payment Devices Frauds Act No. 30 of 2006 were enacted to have certainty in the electronic payment systems and to preserve their integrity. The Computer Crimes Act No. 24 of 2007 provides for the identification of computer crimes and stipulates the procedure for the investigation and enforcement of such crimes. The applicable provisions related to evidence are stipulated primarily in the Evidence Ordinance and on the admissibility of electronic evidence, Evidence (Special Provisions) Act No. 14 of 1995 and Electronic Transactions Act No. 19 of 2006 are the two statutes applicable in Sri Lanka. This study aims to identify the extent of the authenticity, strength and challenges of digital or electronic evidence in criminal trials, by identifying legislative trends in Sri Lanka and the legal systems of other jurisdictions.

II. DEFINITION OF ELECTRONIC EVIDENCE

Evidence (Special Provisions) Act No. 14 of 1995 and Electronic Transactions Act No. 19 of 2006 of Sri Lanka do not contain any definition of the term electronic evidence. As defined by the Council of Europe, electronic evidence or digital evidence may take the form of text, video, photographs or audio recordings. Data may originate from different carriers or access methods, such as mobile phones, webpages, onboard computers, or GPS recorders, including data stored in a storage space outside the party's own control.[4] One

* Judge of the High Court of Sri Lanka and the Deputy Director of the Sri Lanka Judges' Institute, Sri Lanka.

[1] Digital 2022 Sri Lanka <https://datareportal.com/reports/digital-2022-sri-lankaaccessed > accessed 5 Jun. 2022.

[2] CERT Annual Activity Report<www.cert.gov.lk/Downloads/General/Sri_Lanka_CERT_Annual_Activity_Report_2020.pdf> accessed 5 Jun. 2022.

[3] Police cautions public about cyber crimes< https://www.newsfirst.lk/2022/02/26/police-cautions-public-about-cybercrimes> accessed on 6 Jun. 2022.

[4] Electronic Evidence <https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5>

of the most significant definitions of "electronic evidence" was given by the Evidence project, which operates under the auspices of USAID, according to which electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential value that are generated, processed, stored, or transmitted using any electronic device. Digital evidence is that electronic evidence that is generated or converted to a numerical format.[5] This definition of electronic evidence has broader applicability than description by the Standard Working Group on Digital Evidence or the International Computer Evidence Organization,[6] as it includes both digitally born evidence and that which in the course of its life is transformed and then stored or exchanged in electronic form.

III. CLASSIFICATIONS OF ELECTRONIC EVIDENCE

Electronic evidence can be categorized into several divisions and classifications according to various criteria.

A. Classification by Type[7]

This includes documents written on a computer, messages written and sent via e-mail, and texts sent by mobile phone or voice recordings. The electronic evidence can be recorded and stored on a cell phone or on an app. Digital photos, either as hard copies printed out or stored digitally, are clear examples of the visual facts of the crime.[8]

B. Classification by Method

Classification by method of data creation was established by the US Department of Justice in 2002.This includes records created with computer software, known as outputs, such as log files, ATM bills, and mobile phone records, records saved by plugging data created by computer programmes and software, inputs processed by Excel calculations, records kept on computer, such as written documents, and saved as word processing files, chat room messages, and saved e-mails.[9]

C. Classification by Purpose

The third category of classifying electronic evidence is according to the purpose for which it was created. Accordingly, electronic evidence is subdivided into two categories. The first is evidence fit to be means of proof.[10] This includes phone bills and computer records, records part of which has been saved in the machine and processed by software. The second subdivision is evidence not prepared as a means of proof. This type of digital evidence is unintentionally left behind by the perpetrator.[11]

IV. CHARACTERISTICS OF ELECTRONIC EVIDENCE

Electronic evidence has characteristics that distinguish it from other traditional forensic evidence, and the most prominent characteristic is electronic evidence being scientific.[12] Such evidence is used to provide valid data and facts that have been presented for proving or denying the culpability of an offender using high-quality science and data to make sure that the evidence can be relied upon by a court of law.[13] Therefore,

---

accessed 5 Jun. 2022.

[5] Biasiotti MA, Cannataci JA, Bonnici JPM, Turchi F (2018) Introduction: opportunities and challenges for electronic evidence. In: Handling and exchanging electronic evidence across Europe. Springer, Cham, Switzerland, pp. 3–12.

[6] Scientific Working Groupe on Digital Evidence <https://www.swgde.org/documents/published> accessed 5 Jun. 2022

[7] Warken, C. (2018) Classification of electronic data for criminal law purposes, vol 4.

[8] Mason S, Seng D (2017) Electronic evidence. University of London Press <https://doi.org/10.14296/517.9781911507079

[9] Abdel-Muttalib MAM (2006) Search and criminal investigation in the digital computer and Internet crimes. National Library.

[10] Moussa, A.F. Electronic evidence and its authenticity in forensic evidence. *Egypt J Forensic Sci* 11, 20 (2021).

[11] Ibid.

[12] See note 6.

[13] See note 9.

each type of evidence is subjected to a test of its validity. This is an implementation of the rule that the law seeks justice or knowledge to elicit the truth. Therefore, electronic evidence presented to a court of law should be based on scientific logic, and there should be no doubt to its validity.[14]

Information technology includes many types of digital data that can be transmitted electronically. Electronic evidence is a link between that data and the crime, and also a link between the victim and the perpetrator.[15] Electronic evidence is analytical and able to monitor important information about the perpetrator and allow forensic specialists to analyse their electronic or digital footprints to identify the movements, habits, and electronic behaviours of a perpetrator. It is required for forensic evidence to be accepted as evidence if it is obtained legally. Investigators are required to collect evidence according to the policies and procedures set by law.[16]

V. CONCEPT OF TRUSTWORTHINESS

Any judge who hears and determines a case involving electronic evidence will certainly consider the trustworthiness of the witnesses and the evidence tendered. There are two qualitative dimensions of the concept of trustworthiness.

- Reliability
- Authenticity

Reliability means to demonstrate that the record can stand for the facts to which it attests. Authenticity means the record is what is claims to be.[17] Reliability and authenticity are conditions precedent to admissibility.[18]

VI. SRI LANKAN PERSPECTIVE

The admissibility of electronic evidence is considered in accordance with the provisions of the Evidence (Special Provisions) Act No. 14 of 1995 and Electronic Transactions Act No. 19 of 2006 in Sri Lanka. Section 4 of the Evidence (Special Provisions) Act stipulates how any contemporaneous recordings are admissible. In a similar manner, section 5 of the said Act stipulates the manner in which any information contained in any statement produced by a computer shall be admissible. In either case, it is a prerequisite to give 45-days' notice before the date fixed for inquiry or trial, in accordance with section 7 of the said act. In the case of *Abeygunawardena vs. Samoon and others*,[19] the Court of Appeal held that compliance with section 4 is mandatory for electronic evidence. In the case of *Attorney General vs Potta Nauffer and others*,[20] the court accepted the computer-generated evidence in respect of telephone call records as admissible as there was sufficient compliance with the provisions of the Evidence (Special Provisions) Act. Section 22 of the Electronic Transactions Act No. 19 of 2006 stipulates the situations where the Electronic Transactions Act is not applicable. Further, section 21 stipulates that the court shall, unless the contrary is proved, presume the truth of the information contained in a data message, or any electronic document. Therefore, it demonstrates that there is a dual regime applicable in Sri Lanka in respect of admissibility of electronic evidence.

[14] Golubtsov VG (2019) Electronic evidence in the context of e-justice. Civil Procedure Bull 9(1):170–188. https://doi.org/10.24031/2226-0781-2019-9-1-170-188

[15] Losavio MM, Pastukov P, Polyakova S, Zhang X, Chow KP, Koltay A, James J, Ortiz ME (2019) The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. Wiley Interdiscip Rev Forensic Sci 1(5):e1337.

[16] Rajan AV, Ravikumar R, Al Shaer M (2017) UAE cybercrime law and cybercrimes – an analysis. In: 2017 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, p. 1-6.

[17] Heather MacNeil, Trusting Records, Legal Historical and Diplomatic Perspectives- Kluwer Academic Publishing 2000.

[18] Daniel K.B. Seng, Computer output as evidence, 1977 sing JLS 161-3

[19] 2007 I SriLR 276.

[20] 2007 2 Sri LR 144.

The United Nations Office on Drugs and Crime has formulated a module[21] for Digital evidence admissibility, assessment, consideration and determination.[22] This module consolidates common legal and technical requirements for evidence admissibility across jurisdictions. More importantly, this module paves the way for standardization of digital forensics practices, which is key to ensuring the admissibility of digital evidence across different jurisdictions. *Taking in to account the transnational nature of cybercrime, such a harmonization of digital forensics practices is not only of paramount importance to the investigation of cybercrime, but is also essential to international cooperation on cybercrime matters.*[23]

It will be crucial to see how the evidence collected after the Easter Sunday Attacks, May 9th Incidents and the evidence found in social media is presented to court as electronic evidence.

VII. CONCLUSION

The study leads to the conclusion about the need for the adoption of international agreements on harmonization of digital forensic practices to preserve electronic evidence from destruction and vandalism, and obligate countries to implement and abide by these agreements.

In order to achieve ultimate results from adopting uniform digital forensic practices, capacity-building of those responsible for investigating and prosecuting crimes related to computer and information technology must be implemented continuously. Further, it is also necessary to develop capacity-building programmes for judges on assessing electronic evidence, focusing on the technological aspects of electronic crime which would enable the justice professionals to find the perpetrators of cybercrime and obtain evidence to convict them.

[21] https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html

[22] Albert Antwi-Boasiako, Hein Venter. A Model for Digital Evidence Admissibility Assessment. 13th IFIP International Conference on Digital Forensics (DigitalForensics), Jan 2017, Orlando, FL, United States. pp. 23-38, ff10.1007/978-3-319-67208-3_2ff. ffhal-01716394f

[23] Ibid.