BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 15, NUMBER 7 (2022)
ISSN 2029-0454

Cite: *Baltic Journal of Law & Politics* 15:7 (2022): 1352-1360
DOI: 10.2478/bjlp-2022-007098

Admissibility Of Electronic Evidence In Malaysia

Anita Harun
Faculty of Law, Universiti Kebangsaan Malaysia (UKM).

Ramalinggam Rajamanickam
Associate Professor, Faculty of Law, Universiti Kebangsaan Malaysia (UKM)

Insyirah Mohamad Noh
Faculty of Law, Universiti Kebangsaan Malaysia (UKM)

Received: October 24, 2022; reviews: 2; accepted: December 08, 2022

Abstract

This paper aims to examine the legal framework for the admissibility of electronic evidence and to identify the issues relating to computer or electronic evidence and its application in Malaysian courts. Enactments of new legislation to accommodate cyber-crime cases and amendment to section 90A, 90B and 90C of Evidence Act 1950 provided for the admissibility of computer-generated documents. This raises the question on the admissibility as evidence of a computer-generated documents in court. Another issue with computer-generated evidence is that it can be easily altered without leaving any glaring trace of its alteration. Hence, rules for admissibility and the probative or prejudicial value to be attached to such evidence need to be addressed. The method of study conducted is a pure legal study which is categorized as doctrinal research. This doctrinal research use a qualitative approach that involved the use of several integrated approaches. There are references made on primary and secondary evidence and among the approaches used in this study are critical analysis and content analysis. At the end of this paper, there are discussions and comparison from other jurisdictions in order to improve the position of computer-generated evidence and its application in Malaysia.

Keywords

cyber-crimes, electronic evidence, section 90A Evidence Act, computer generated document, admissibility as evidence

Introduction

In New Straits Times report dated 6 November 2019, Deputy Home Minister Datuk Azis Jamman in the Dewan Rakyat said that scammers via online scams raked a whopping RM 186,027,122.72 from their victims in the first eight months of that year. The amount was from 3,533 cases recorded between January and August 2019. The number of online scams recorded nationwide for 2018 stood at 4,956 cases and involved a total loss of RM 224,653,895.18 (Yusuf, 2019).

Modern technology has dramatically changed the way information is created, transmitted, processed, and stored (Mason, S. & Seng, D., 2017). Each wave of the digital revolution brings novel challenges to the legal world. A peculiar breed of offences involving the abuse and misuse of information using technology - often broadly described as cybercrimes - has emerged. New methods of conducting litigation have surfaced in courtrooms (Khisamova et. al, 2019).

Cybercrimes is a computer crimes or high-tech crimes which were committed by individuals that intended to either destroy other's property, personal integrity or life or to steal other people's valuable property and information (Mohamed, 2013). Some of crimes that can be included as cybercrime are spreading computer viruses, committing denial of service attacks ('DOS'), sending phonographic materials, committing unauthorised access or hacking, committing unauthorised modification of computer data, mass web defacement, committing phishing (Chia, L. et. al, 2021) or identity theft (Ahmad, 2013), cybersquatting, cyber stalking (Global Legal Group, 2018) and many others. These crimes never halt and will continue to expand as a result of the development of technology (SKMM, 2021).

Commercial Crime Division of Royal Malaysian Police (PDRM) classified cyber-crime cases into three categories, namely content offenses, computer crimes and cyber-fraud. Content offences are to include slander, obscenity, sedition and threats. Computer crimes cases are for example hacking, malware and Ddos. Cyber fraud to include phishing, parcel scam, spoofing, e-shopping and e-mail scams (Pitchan, M., A. et al, 2017).

The range of criminal activities escalated as a result of the advent of cyber-crimes (Halen, 2015). Cybercrimes can be committed on a far broader scale than their traditional, real-world counterparts (Tang, C. F., et al, 2015). A criminal can commit theft, extort victims, plan a robbery, vandalize property, solicit prostitutes, and bully, harass, and stalk a target in the privacy of his or her own home by using the internet and the right technology. A recent statistic by PDRM show an increase in the numbers of reported cyber-crimes case (Meikeng Y., 2020).

Research Methodology

This is a study of pure legal research categorized as a doctrinal study. The materials referred consisted of both primary and secondary sources, such as the statutes, decided cases, textbooks, articles, journals, papers and other related

publications. Furthermore, in this research, author used qualitative approaches, which may involve the use of multiple integrated approaches. Among the approaches used in this study are critical analysis, content analysis as well as descriptive methods. Critical analysis is used because the texts and scientific materials obtained from the library study are critically evaluated and researched by the authors. In addition, the author also uses content analysis related textbooks, articles and decided cases.

Admissibility Of Evidence Under Section 90a Of Evidence Act1950

Legislative Framework

The starting point is section 90A of the Evidence Act 1950, inserted in 1993 to provide for the admissibility of documents produced by computers and of statements contained therein.

The section 90A does not adopt the neutral term "electronic evidence" or "digital evidence", as is favoured in other jurisdictions, preferring the specific phrase "a document produced by a computer". Nevertheless, both "document" and "computer" are given wide definitions in the Evidence Act 1950. In the Computer Crimes Act 1997 (Act 563) –

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

"computer network" means the interconnection of communication lines and circuits with a computer or a complex consisting of two or more interconnected computers;

"computer output" or "output" means a statement or a representation whether in written, printed, pictorial, film, graphical, acoustic or other form—

(a) produced by a computer;

(b) displayed on the screen of a computer; or

(c) accurately translated from a statement or representation so produced;

"Document" comprises any matter expressed, described, or howsoever represented, upon any substance, material, thing or article. The definition of "computer" under section 3 of the Evidence Act was amended in 2012 to ensure consistency with the Computer Crimes Act 1997 to include electronics, magnetic, optical, electrochemical, or any other data processing devices, or a group of such interconnected or related devices, performing logical, arithmetic or storage functions, including a communications facility. The breadth of the term is further underscored by section 90A(5), which states that a document is deemed to have

been produced by a computer regardless of whether it was produced directly or through equipment, and whether any direct or indirect human intervention was involved. The scope of section 90A thus encompasses a myriad of information, ranging from bus tickets to CCTV recordings and DNA test reports. Ahmad Najib bin Aris v Public Prosecutor [2009] 2 MLJ 613, the Federal Court held that CCTV tapes were documents ascribed under definition of section 3 Evidence Act.

In Bergamo Development (M) Sdn. Bhd. v Eck Development Sdn. Bhd. & Anor [2018] MLJU 555, the Court held that a Samsung Galaxy S6 Mobile Phone is a Computer.

'… Consequently and in my opinion, the Plaintiff herein has satisfied the pre-requisites by the tendering of a certificate made pursuant to section 90A(92) Evidence Act 1950 by the director of the Plaintiff who is responsible for the care and management of the usage of the Samsung Galaxy S6 mobile phone (serial no. R58G3246MHV) and Hewlett-Packard laptop computer (serial no. CNF1042Ys7) …

The main provisions may be briefly summarised as follows. Section 90A (1) sets out the condition precedent for a document produced by a computer to be admissible, which is, it must be "produced by the computer in the course of its ordinary use" (Mohamed, D., 2011). A document is admissible as evidence as long as it is produced whether or not it is tendered by its maker. Evidence law has remarked that a document produced by a computer is a primary evidence. For that, the common law hearsay rule has been disregarded by section 90A, which is also a statutory exception to the rule.

To prove that a document was produced by a computer in the course of its ordinary use, a certificate may be tendered to court, signed by a person responsible for the management of the computer's operation, or for the conduct of activities for which that computer was used as prescribed by Section 90A (2) of the Evidence Act 1950 (Pitchan, M., A. et al, 2019). Once such certificate is given, under section 90A (4), the computer is presumed to be operating properly in all respects throughout the period during which the document was produced (Nibras S. K., 2021).

Section 90A (3) provides that the maker of the document is not required to provide the certificate nor the person who gave the certificate to provide oral testimony. According to section 90A (1), any document that has been produced by a computer will be admitted as a primary evidence. However, the court will still have to decide on the reliability and authenticity of the document (Gita, R., 2014).

A computer-generated document shall be regarded as a primary evidence and activate the presumption that the 'çomputer' was in good working order and has operated properly throughout the period during the document was produced once a certificate under section 90(2) is tendered (Nibras S. K., 2021).The evidential burden of disproving would borne by the party challenging its credibility if the contents of the certificate are to be challenged (Mohamed, D., 2013).

Section 90A (6) states that a computer-generated document shall be admissible whether or not it was produced after the commencement of any investigation or proceedings. Such a document shall be deemed to be produced by

the computer in the course of its ordinary use. Pursuant to section 90C, section 90A is accorded precedence and prevails over any inconsistent provision in any written law regarding the admission of evidence (Mohamad, A. M., 2019).

Application of Section 90A of Evidence Act 1950

The statutory requirements for admissibility in section 90A have not been strictly interpreted. On the contrary, the approach by the courts suggests a gradual loosening of the requirements, based on the notion that section 90A was intended to facilitate rather than obstruct the admissibility of computer-generated documents.

The first inroads were made when the Court of Appeal in Gnanasegaran a/l Pararajasingam v Public Prosecutor [1997] 3 MLJ 1, held that it is not mandatory to tender a certificate under section 90A (2) in every case. The words "may be proved" were read to indicate that a certificate is not the only means of proving that a document is produced by a computer in its ordinary use. In lieu of producing a certificate, the prosecution may adduce oral evidence through a witness. Such oral evidence must state that the document was produced by a computer in the course of its ordinary use and was in good working order and was operating properly in all respects throughout the period during the production of the document (Pitchan, M., A. et al, 2019).

The oral evidence need not be given by a person responsible for the management and operation of the computer concerned. It is sufficient if the witness is familiar with the operation of the computer, has some knowledge of what the computer is required to do, and is able to say it is doing it properly (Casey, E., 2011). Hence, the court accepted the evidence of an auditor, who did not operate a bank's computer but who had access to view the documents it produced, that such documents were produced by a computer in the course of its ordinary use (Mohamed, D., 2011).

Notably, courts have been willing to admit computer-produced documents even in the absence of either a certificate or oral evidence that it was produced in the ordinary use of the computer. In Ahmad Najib bin Aris v Public Prosecutor [2009] 2 MLJ 613 at [33] (FC), the Federal Court drew a distinction between sections 90A (1) and (6): the former governed the admissibility of documents produced by a computer in its ordinary use, whereas the latter was a deeming provision aimed at documents produced by a computer not in its ordinary use. On the facts, there was neither a certificate nor oral evidence that a chemist report was produced in the ordinary use of a computer. The Federal Court heled that there were two ways of tendering documents produced by a computer under section 90A (1). The chemist report was admitted because of detailed oral testimony on the course of its ordinary use and maintenance. Since the only available evidence is that the report was generated by a computer, it was appropriate to resort to section 90A (6) to presume that it was produced in the course of ordinary use, thus rendering the report admissible.

In Public Prosecutor v Azilah bin Hadri & Anor [2015] 1 MLJ 617, the Federal Court decided that the documents produced by a computer sought to be relied upon by the prosecution were admissible although the requirements of section 90A of the Evidence Act 1950 had not been complied with as long as the makers of the documents were called or such documents were admitted under any other established exception to the rule against hearsay.

More recently in Lau Chee Kai v Public Prosecutor [2016] 6 MLJevi 223 at [28] CA, the document in question was a computer printout consisting of serial numbers of bank notes, keyed in by two individuals. No certificate was tendered under section 90A (2). Only one of the two individuals were called to give evidence, and she did not state whether the document was produced by a computer in the course of its ordinary use. The Court of Appeal held that the document was nevertheless admissible under section 90A (6). With this development, the basic requirement in section 90A to prove that a document was produced by a computer "in the course of its ordinary use" - whether by a certificate or otherwise - has been all but discarded.

It was once thought that section 90A is "the only law under which all documents produced by a computer are to be admitted in evidence". However, the Court of Appeal in Mohd Khayry bin Ismail v Public Prosecutor [2014] 4 MLJ 134 at [30] (CA), stressed that the insertion of section 90A did not displace common law principles on admissibility. A tape recording is admissible at common law based on res gestae principles, and if it is relevant and its accuracy established to the satisfaction of the court. As such, a CCTV recording was found to be admissible by applying common law principles, despite the lack of any certificate or oral evidence to the effect that the recording was produced in accordance with section 90A(1).

The effect of these developments is that while the statutory requirements in section 90A have been significantly watered down, the existing common law rules of evidence continue to apply generally in respect of computer-produced documents. It may be queried what, if any, practical significance is left of the specific legislative scheme in section 90A.

A Return To General Principles

The wide scope of "documents produced by a computer" under section 90A entails a broad-brush approach. Section 90A creates a new category of primary evidence on the basis that a computer was involved in the production of the document. It makes no distinction between the multifarious functions of a computer in the production of a document. In any particular case, the computer may be used:

Merely as an electronic filing cabinet to store data manually entered by a person (for instance, Excel spreadsheets);

To collect and record data automatically (telephone call logs); or

To interpret or analyse data entered by external sensors to generate results (breathalyzer).

The section treats a broad spectrum of computer-produced documents as a single homogenous category and renders them admissible without the need to call the maker of the document. This may produce incongruous results. For type (i) documents above, what may have been inadmissible as documentary hearsay if written on paper without the maker being called to give evidence, would become admissible if entered and saved onto a computer.

In light of the inherent difficulties in formulating and applying special rules for electronic evidence, it is perhaps unsurprising that provisions similar to section 90A has been repealed in other jurisdictions. Similarly in Singapore, the original section 35 of the Evidence Act (Cap 97) provides for three modes to admit computer output, namely by agreement of parties, by production through an approved process, or by proof that the output is accurate and reliable, having been produced by a computer that has been properly operated and used (Yunus, M. I. M., 2006). The supplementary provisions in section 36 relate to the calling of further evidence where the Court is not satisfied as to the accuracy of the computer output. Both sections have since been repealed by section 7 of the Evidence (Amendment) Act 2012 as follows –

Facts which are the occasion, cause or effect of facts in issue

7. Facts which are the occasion, cause or effect, immediate or otherwise, of relevant facts or facts in issue, or which constitute the state of things under which they happened, or which afforded an opportunity of their occurrence or transaction, are relevant.

The explanatory note to the amendment bill elaborated that the non-computer specific approach is "based on the principle of non-discrimination, which requires that electronic evidence be treated no differently from evidence not in electronic form". Existing rules on relevancy and admissibility (including hearsay, the best evidence rule, and rules on authentication) will apply equally to electronic evidence as to any other evidence. Courts are given a discretion to call for evidence as to authenticity as they deem appropriate (Inbrief, 2017). Full flexibility is preserved by avoiding the prescription of express requirements for electronic evidence.

Given that the case laws on section 90A appear to be headed in the same direction, it is timely to ask whether the continued application of the section merits reconsideration.

Conclusion

Electronic evidence has unique characteristics that differentiate them from more traditional forms of evidence. It is vulnerable to alteration often without leaving any obvious trace. Content may be lost in the transfer of evidence from one format or medium to another. In some instances, the very act of opening a file may trigger changes to it through prior programming. With increased sophistication in the realm of cyber-crime, electronic evidence may no longer be presentable in the form of computer printouts; hidden information and ghost or

deleted files are not easily accessible or obviously readable. In light of the relatively low threshold in section 90A, the main challenge lies not in admissibility but the authenticity of electronic evidence.

As aptly observed by the US District Court in Verizon Directories Corp v Yellow Book USA, Inc (2004) 331 F Supp 2d 136:

"Computer technology is like the proverbial genie that has come out of the bottle. Stuffing it back inside is unlikely. It can be an instrument for good or a weapon of prejudice and manipulation. The courts will have to harness this unbound energy and set rules for its appropriate use in the courtroom. And appellate courts will have to accept yet another burden, meaningful policing of the new genie."

References

Chia, L. & A. (2021). Basics of Cyber Security Law in Malaysia.

Eoghan Casey. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed.). Elsevier Inc.

InBrief. (2017). Computer and Digital Evidence in Criminal Trials.

Khisamova Z.I, Begishev I.R, Sidorenko, E.L. (2019). Artificial Intelligence and Problems of Ensuring Cyber Security. International Journal of Cyber Criminology, 13(2), 564-577.

Global Legal Group. (2018). The International Comparative Legal Guide to: Cybersecurity 2019 (4th ed.). Global Legal Group.

Mohamad, A. M. (2019). Admissibility and Authenticity of Electronic Evidence in the Courts of Malaysia and United Kingdom. International Journal of Law, Government and Communication 15, 4(15), 121–129.

Mohamad Ismail Mohamad Yunus. (2006). Kedudukan Bahan Bukti (Exhibit) Elektronik Dan Digital Dalam Keterangan: Masalah Dan Cabaran Masa Kini. Insaf: The Journal of the Malaysian Bar, 35(1), 1–14.

Mohamed, Duryana. (2011). Computer Evidence: Issues and Challenges in the Present and in the Future. Current Law Journal, 67.

Mohamed, Duryana. (2013). Combating the threats of cybercrime in Malaysia: The efforts, the cyberlaws and the traditional laws. Computer Law Review & Security Review, 29, 66–76.

Muhamad Asyraf Ahmad Terimi et. al. (2013). Jenayah Siber: Pengelasan di antara Al-Jaraim dan Al-Jina'I menurut Sistem Perundangan Islam. International Seminar on Islamic Jurisprudence in Contemporary Society, 539–551.

Muhammad Adnan Pitchan et. al. (2017). Analisis Keselamatan Siber dari Segi Perspektif Persekitaran Sosial: Kajian Terhadap Pengguna Internet di Lembah Klang. Journal of Social Sciences and Humanities, 2(12), 16–29.

Muhammad Adnan Pitchan et. al. (2019). Dasar Keselamatan Siber Malaysia: Tinjauan Terhadap Kesedaran Netizen dan Undang-Undang. Jurnal Komunikasi: Malaysian Journal of Communication, 35(1), 103–119.

Nibras Salim Khudhair. (2021). Revisiting the Admissibility of Electronic Evidence: Indian Jurisdictions & Notes from Other Countries. Psychology and Education, 58(5), 1135–1148.

Radhakrishna Gita. (2014). Distinguishing Between Admissibility and Authenticity of Electronic Evidence. Malayan Law Journal, 6(35), 1–14.

Stephen Mason, & Daniel Seng. (2017). Electronic Evidence (4th ed.). LexisNexis Butterworths.

Suruhanjaya Komunikasi dan Multimedia Malaysia. (2021). Perundangan.

Chor Foon Tang, & Sezali Md. Darit. (2015). Penentu Makroekonomi Kadar Jenayah di Malaysia. Jurnal Ekonomi Malaysia, 49(2), 53–60.

Yuen Meikeng. (2020). Cybersecurity cases rise by 82.5%. The Star.