Technology-Based Crimes in Malaysia: Issues and Challenges for Investigation Officers in Gathering Computer Evidence

Bromeley Philip

Academy of Language Studies, University Technology Mara (UiTM) Sarawak

DOI : https://dx.doi.org/10.47772/IJRISS.2024.8110263

Received: 15 November 2024; Accepted: 19 November 2024; Published: 23 December 2024

ABSTRACT

Technology advances faster than law and thus, the legislation must be broad enough in order to be able to embrace future technological development particularly in regard to the issues relating to gathering of evidence for trial. This paper discusses how the investigating officer (IO) gathers evidence from computers involving technology-based crimes committed both in the real world as well as the cyberspace, and whether it needs to be carried out within the scope of conventional legal framework of Evidence Act (EA) 1950, the Criminal Procedure Code (CPC) and Penal Code per se or there are other legal regimes that specifically allocate the right provisions for those crimes. This is to ensure that specific crime be charged under specific Act accordingly. There is the Computer Crimes Act 1997 (CCA 1997), with its main focus on the function of the device. For a device to fall under the definition of a computer, it must be capable of performing the functions of a computer. Other Acts include the Communications and Multimedia Act 1998 (CMA) and the Mutual Assistance in Criminal Matters Act 2002 (MACMA). With these Acts available, the key question addressed in this paper is, what are the real issues and challenges faced by IOs in gathering evidence especially for those crimes whose evidences are stored in computers, or cybercrimes for that matter. The paper concludes that for an IO to meet emergent issues and challenges, he needs to work within the scope of all those Acts to gather evidence in for any criminal prosecution involving computer/cybercrimes. In recent years, IO needs to understand how Artificial Intelligence (AI) works in the context of criminal investigations.

Key words: computer; digital; cybercrime; evidence; artificial intelligence

INTRODUCTION

In recent years, the advancement of technologies has inevitably put more challenges on law enforcement agencies particularly with regard to issues related to gathering of evidence for trial. Criminals are increasingly technology-savvy, thus making the process of gathering evidence a complicated and demanding task for the investigating officers as a conventional process may not be sufficient anymore. Technology advances faster than law and thus, the legislation must be broad enough to be able to embrace future technological development particularly in regard to the issues relating to gathering of evidence for trial. Several questions need asking namely, for technology-based crimes which involve the use of computers to commit crimes both in the real world as well as the cyberspace, can the investigating officer (IO) gather evidence from computers within the scope of conventional legal framework of Evidence Act (EA) 1950 and the Criminal Procedure Code (CPC) per se? Are these two legal provisions adequate to embrace the nature and scope of the new types of crimes? While it is clearly outlined in the CPC all the necessary steps and procedures to follow in gaining access to the crime scene for conventional crimes to process evidence; are similar steps and procedures suitable and thus applicable to gaining access to a computer to retrieve digital evidence? What other new or existing laws are made available as points of reference to conduct criminal investigation in relation to gathering of electronic evidence from computers or electronic devices?

Indeed, such new form of evidence as stored in computers or electronic devices require new laws and digital forensic investigation process that differ in some ways from the traditional criminal investigation process particularly in terms of accessing digital evidence in computer storage. New laws or existing laws need to be amended to make provisions to enable criminal investigation into retrieving the digital evidence while

simultaneously ensuring its authenticity before it could be presented in the courts for discretionary assessment of its relevance and admissibility. In this respect, the government has introduced practically new cyberlaws which include Computer Crimes Act (CCA) 1997, Communications and Multimedia Act (CMA) 1998 and Digital Signature Act (DSA) 1997. Are these CCA 1997, CMA 1998 in addition to the traditional CPC and EA 1950 adequate to assist the investigating officers in gathering sufficient evidence? It must be remembered that for the prosecution to succeed the IO must have provided relevant and admissible evidence by virtue of the EA 1950 to be accepted by the courts. The onus is on the investigating officers (IOs) to ensure that they adhere closely to the steps and procedures as stated in the provisions both in those Acts as well as CPC, the Penal Code and EA 1950 to collect digital evidences that are relevant and admissible accordingly. Working closely with the prosecutor the investigation officer must critically ensure that the digital evidences gathered are authentic, relevant and hence admissible in order to first establish a prima facie case against the criminal suspect. For the prosecutors in particular, they must make sure that not only are the evidences gathered by the IO relevant and admissible in court, but that the chain of evidence must not be broken.

LITERATURE REVIEW

This article is a discussion paper. The paper will look into legal literature to explore what constitutes computer evidence as defined and recognised by the laws in Malaysia first. Next it will look into some decided court cases involving computer evidence to see how the existing laws were used in admitting or rejecting computer evidence. Subsequently, the discussion will then focus on the challenges faced by IOs in gathering digital evidence as far as computing skills and knowledge are concerned; what makes it difficult for instance, to trace and authenticate digital evidence?

Relevancy and Reliability

For electronic or computer evidence, relevancy and reliability are two important criteria for admission. These two criteria are sometimes very difficult to determine due to the fact that the evidence in a computer may be connected to various computer networks and may be tampered with. Furthermore, the reliability of computer evidence starts with a combination of two elements namely, trustworthiness of the content of a piece of computer derived evidence and trustworthiness of the process by which it was produced (Brenner, 2005). The admissibility of evidence could be challenged by attacking the weight or reliability of the evidence. Nonetheless, what is very pertinent before critically analysing the challenges faced by IOs in gathering computer evidence is to determine the position of computer evidence in the context of existing current laws in Malaysia.

Computer Eevidence under Malaysian laws

Computer evidence is data from computer systems that is used as evidence in legal proceedings. It exists when a computer is used by any person to do his works, to access other person's computer or to communicate with others. This data is kept in the hard drives of the computer system and available in different software programs. It will remain in the computer until it is removed, deleted or rewritten. The data is used as evidence in a variety of cases including cases of computer misuses, conspiracy, murder, rape, breach of online contracts, internet defamation and many others. This data will be retrieved, analysed and used as evidence to prosecute and charge the suspects. This electronic evidence is used it will include computer generated evidence, computer produced evidence, computer printout, computer output, computer-based evidence, computer-related evidence, electronic data and electronic document (Duryana Mohamed, 2011).

Documentary Evidence

According to section 3 of the Evidence Act 1950 'computer' means,

'Any device for recording, storing, processing, retrieving or producing any information or other matter, or for performing any one or more of those functions...,' While section 2(1) of the Computer Crimes Act 1997 (CCA 1997) defines the term 'computer' as,

'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....'

Based on the above two definitions it is submitted that the definition given by the Evidence Act 1950 extends the scope of the term 'computer' by looking at the ability of the device. Any device is regarded as a computer if it is capable of recording, storing, processing, retrieving or producing information. Any networking or combination of functions between two or more computers is considered as a single computer.

Computer Crimes Act 1997

While for the CCA 1997, the main focus is on the function of the device. For a device to fall under the definition of a computer, it must be capable of performing the above functions. In short, the definition under the CCA is more technical and it limits the scope by excluding automated typewriter or typesetter, a hand calculator and non-programmable device from being a computer.

Other than the EA 1950 and the CCA 1997, the Penal Code of Malaysia also mentions the word 'computer' in illustration to section 29. Section 29 explains about the meaning of document and it includes 'a matter recorded, stored, processed, retrieved or produced by a computer.' As for the word 'electronic' it is defined by section 5 of the Malaysian Electronic Commerce Act 2006 as 'the technology of utilizing electrical, optical, magnetic, electromagnetic, biometric, photonic or other similar technology'. This definition focuses on the technology of utilizing various technological devices and does not specifically mention about computer. It refers to the application of technology in electronic commerce.

Definition under Evidence Act 1950

The definition given by the Evidence Act 1950 is more general and shall be applicable to any type of computer related cases. As for 'computer output', most cases discuss its admissibility under sections 90A, 90B and 90C of the Evidence Act 1950: 'any device for recording, storing, processing, retrieving or producing any information or other matter, or for performing any one or more of those functions…' In Malaysia, computer evidence is admissible as documentary evidence and primary evidence. This fact is established based on sections 3 and 62 of the EA 1950. Furthermore, the admissibility of computer output is also established under sections 90A, 90B and 90C of the EA 1950. Section 90A requires the production of the printout from the computer in the course of its ordinary use. It also emphasises on the status or position of the person who makes or tenders the document and the requirement that the certificate must be signed by a person responsible for the management of the operation of that computer or for the conduct of the activities for which the computer was used. If the person responsible for that computer is present then the certificate is not required as oral testimony of that person is sufficient and shall be admissible as evidence (Duryana Mohamed & Zulfikar Ramlee, 2014).

On the other hand, section 90A (6) deals with the admissibility of a document which was not produced by a computer in the course of its ordinary use and is only deemed to be so. This section can only apply to a document which was not produced by a computer in the ordinary course of its use, or, in other words, to a document which does not come within the scope of section 90A (1). Thus, it cannot apply to a document which is already one that is produced by a computer in the ordinary course of its use. The document must be proved in the manner authorized by section 90A (2). It can now be discerned with ease that section 90A (6) has its own purpose to serve and can never be a substitute for the certificate.

Section 90B focuses on the weight to be attached to a document, or a statement in a document, admitted by s. 90A. These include the manner and purpose of the creation as well as the accuracy of the document, the interval of time between the occurrence or existence of facts mentioned and also the supply of the information including the real intention of the person who supplies or had custody of the document. Section 90C further affirms the position of ss.90A and 90B. This section implies that the admissibility of computer printouts in Malaysia under ss.90A and 90B shall be determined by the EA 1950 only and not by any other written laws, locally or abroad.

Issues on computer evidence: Malaysian cases

The Evidence Act 1950 (EA1950) was amended in 1993 to facilitate the admission of computer-generated

evidence based on the prevalent belief that the unique nature of computer evidence necessitated special treatment under the law of evidence. The relevant provisions, sections 90A, 90B and 90C EA1950 were based on the English section 5 Civil Evidence Act 1968 (CEA1968). Section 90A with seven subsections, is the principal section governing the admissibility and proof of documents produced by a computer. Section 90B contains guidelines on the probative value to be attached to the evidence, while section 90C, stipulates that the provisions of sections 90A and 90B shall prevail over any contradictions in any other statutes.

In PP v Hanafi Mat Hassan, an automated bus ticketing machine, a thermal cycler and a DNA analyser were found to be 'devices for recording, storing, and producing information' within the ambit of the definition of 'computer' in section 3 EA 1950. Where more than one computer was involved in its production these were recognised and treated as a single computer under section 3 EA 1950 (Radhakrishna, 2016).

Sections 3 and 62 of the Evidence Act 1950 in Malaysia provide the admissibility of digital records as documentary and primary evidence (Act 56). "Computer," as defined in Section 3 of the provision, is an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of interconnected or related devices, that performs logical, arithmetic, storage, and display functions, and data storage facilities or communication facilities that are directly linked to or operate in conjunction with certain interconnected or related devices or groups of devices are included, but automatic typewriters or typewriters are not included, or non-programmable portable hand-held calculators or other similar devices without data storage facilities 'and on the highlighted illustrations, items documented, stored, processed, retrieved, or generated by a computer are documents' (Nurul Syazwani et.al., 2021).

When is a document 'produced' by a computer?

In Approfit Sdn. Bhd. v Kent Sing Construction Sdn. Bhd. & Ors., in determining whether an automated cashier's receipt was a document 'produced' by a Justice Richard Malanjum, opined that only certain categories of documents where there is no human intervention such as bank statements as in Gnansegaran a/l Pararajasingam v PP, were captured by section 90A. More specifically, 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 (Anita, Ramalinggam & Insyirah, 2022).

By the provisions of Section 90A (5), a document is deemed to have been produced by a computer, directly or indirectly, whether or not there was any direct or indirect human intervention. Section 90A (6) provides a further presumption in relation to a document, whether produced by a computer or not (Radhakrishna, Myint Zan & Khong Wye Keen, 2013):

A document produced by a computer, or a statement contained in such document, shall be admissible in evidence whether or not it was produced by the computer after the commencement of the criminal or civil proceeding or after the commencement of any investigation or inquiry in relation to the criminal or civil proceeding or such investigation or inquiry, and any document so produced by a computer shall be deemed to be produced by the computer in the course of its ordinary use.

Print outs of digital photographs from a digital camera were accepted as 'documents produced by a computer' in Bank Pembangunan Malaysia Bhd v. Sasacom Sdn Bhd & Another Case. However, in Avnet Azure Sdn Bhd v Eact Technologies Sdn Bhd and Sapura Research Sdn Bhd., the High Court rejected an email as a document 'produced' by a computer. 'Produced' by a computer, referred to input of data which would be recorded, stored, analysed or processed through some software programme as 'computer output'. For this and other reasons the email was held to be inadmissible and the certificate tendered under section 90A (2) EA 1950 was rejected.

In Hanafi bin Mat Hassan v PP, the Court of Appeal explained that what was relevant for the prosecution was not that the document was 'produced' by the computer, but the statements contained in it. Section 90A required proof of the correct working condition of the computers that produced the results as opposed to the computer that merely recorded it. Although the prosecution did not lead evidence on this, the cross-examination of witness

PW (Prosecution Witness)11 was sufficient to establish this issue. This witness, PW11, explained that the maintenance of the DNA analyser and the thermal cycler was to ensure their good working order, the method of sample analysis to avoid errors, and that the machines were also programmed for self-testing to ensure optimal operational efficiency. The requirements of section 90A (1) were thereby satisfied (Radhakrishna, 2016).

In Microsoft Corporation v Conquest Computer Centre Sdn Bhd., a copyright infringement case, the defendant tendered certain Internet print-outs in reliance of its contention that it had been given a 'trial version' of the software for free use over a period of time and submitted a certificate under section 90A (2). Although the Court admitted the Internet printouts it found no evidence of the defendants' contention of 'right to free use' indicating that the 'weight' is for the judge to assess. A distinction was correctly drawn between the admissibility and authenticity of evidence, something which is not always appreciated (Radhakrishna, 2016).

Proof of ordinary use

Although section 90A EA 1950 does not explain what amounts to 'ordinary use' section 90A (2) provides that this may be proved by a certificate from someone responsible for the management or conduct of activities on that computer that the document was produced in the 'ordinary use' of the computer. It is for the declarant to describe what amounts to 'ordinary use' in a given case. Once this is satisfied, the subsection provides a rebuttable presumption of fact that a document was produced by a computer 'in the course of its ordinary use'.

In PP v Ong Cheng Heong, two computer printouts from the registration department for vehicles were rejected by the High Court as the witness did not claim any responsibility "for the conduct of the activities of the computer'. Thus, the issue of reliability of the document has to be addressed through the reliability of the system that produced it which could be proved by either the contents of the certificate or the oral testimony of a witness (Radhakrishna, 2016).

Is a Certificate mandatory?

The Court of Appeal in Gunasegaram Pararajasingam v PP, went to great lengths to examine and clarify the provisions of section 90A EA1950. Shaik Daud Ismail JCA clarified that under section 90(A)(1) there were two ways of proving 'in the course of its ordinary use' in order to admit 'documents produced by a computer' into evidence:

1. It may be proved by the production of the certificate. This is permissive and not mandatory.

2. By calling the maker of the document which is the usual method to admit and prove any form of documentary evidence.

When should the Certificate Be Tendered?

In Standard Chartered v Mukha Singh, the High Court held that unless the admissibility of the documents were challenged at the time of tendering, it was not necessary to produce the certificate under section 90A(2) EA.30 This was confirmed by the Court of Appeal in Chua Boon Hong v PP. Similarly, in Schmidt Scientific Sdn Bhd v Ong Han Suan, a certificate relating to computer-produced documents contained in a party's bundle of documents tendered subsequently through a witness was held admissible for lack of challenge at the material time. Under section 90A (3) there is no requirement for the maker of the document to provide the certification or for the person who gave the certificate to testify. The reliability, integrity and authenticity of the document is for the judge to decide.

All these cases indicate that the existing EA 1950, CCA 1997 as well as the CPC albeit not specific as regards the definition of computer evidence, still can be used by IOs and prosecutors as the relevant laws in criminal prosecution involving computer evidence. As far as the laws are concerned, the IOs and prosecutors need to be very familiar so as to ensure that any evidences collected are relevant, reliable, authentic and thus admissible. Having explained what is computer evidence in legal terms and how the courts decide on the admissibility of computer evidence, it is necessary to look at the issues and challenges faced by IOs in criminal investigation involving computer evidence to provide a complete picture (Radhakrishna, 2016).

Issues and challenges for IOs in gathering computer evidence

The common issues and challenges faced by investigating officers, prosecutors and even defence counsels are in terms of firstly, locating computer evidence itself, secondly, recovery and discovery of computer evidence and the right to privacy, thirdly, development of new technology and new crimes, fourthly, proving the reliability, authenticity and accuracy of computer evidence, fifthly, multiple jurisdictions, finally, the law may be outdated and reliance on the case law.

Locating data or evidence

Firstly, locating data or evidence can be challenging since the data are created and stored in various places. The data can also be sent from various devices that may contain complex as well as large amount of data. These devices include desktop computer, laptop, Unsecured public Wi Fi, secured Public Wi Fi and VPN (Virtual Private Network). A portable music player such as iPod is also one of the devices that will challenge the investigator's skills and knowledge as well as the forensic expert in locating the evidence of crimes. The issue is how to locate the evidence and what is the appropriate law governing the process of retrieving data from such devices?

If the case is criminal in nature, the Investigating Officer (IO) with the assistance of the computer forensic expert will do the investigation and detection of computer evidence before the retrieval of data from the seized computer. The IO is allowed to do so under the Criminal Procedure Code (Chapter XIII of the CPC), the Computer Crimes Act 1997 (ss10 and 11 of the CCA), the Communications and Multimedia Act 1998 (ss245 to 262 of the CMA) and the Digital Signature Act 1997 (ss76 to 81 of the DSA). The IO may also do the investigation with or without the search warrants. However, with the search warrants the police may access the premise of the suspect and seize the computer belonged to him.

Nevertheless, the challenge to the IO and computer forensic expert is that they must ensure there is no break in the chain of evidence collected. Proper security procedures and mechanisms are needed to protect the integrity of the computer during the gathering of computer evidence. In other words, the evidence collected should be properly preserved, remain original and authentic. These criteria are very important for the admissibility of computer evidence in the court of law.

In relation to the procedures, the Criminal Procedure Code is the main legislation to govern the procedural aspect of criminal investigations in Malaysia. To cope with the advancement of the digital era, new provisions have been introduced to govern the search and seizure of digital evidence in 2012. Due to the lack of any provision that specifically deals with search and seizure of digital evidence, the Parliament of Malaysia passed a new provision, that is section 116B of the Criminal Procedure Code, to deal with this matter. Along with the introduction of section 116B, sections 116A and 116C are also introduced.

Section 116 generally provides for the powers of search and seizure of the police. The section also relates to the summons for production issued under section 51 of the Code. Section 116A further enhanced the power of search without any warrant. The search and seizure without warrant give the police the powers to take possession of any book, document, record, account or data, or another article; or inspect, make copies of, or take extracts of the book, document, record, account, or data, or other article seized. The word "data" here refers to any data held on a computer or any digital device. (Zainal Amin Ayub, Mohamad Fateh Labanieh & Harlida Abdul Wahab, 2023).

Recovery and discovery of computer evidence and the right to privacy

Computer data or any data in electronic medium may be recovered by many ways using specific software. Procedurally, the recovery of data may be made using discovery method. This method of discovery is used to discover relevant documents kept by the other party in his computer or any places and believed to be relevant to the case. In this regard, the parties to the case may either mutually agree to exchange the documents in their possession or may comply with the court order for discovery. Order 24 of the Malaysian Rules of High Court

1980 allows this process even though there is no specific provision on discovery of computer evidence or electronic evidence in the Rules of High Court 198 and other rules of court.

However, caution must be exercised during this process since the parties may challenge on the method used to recover the data. Among the issues are the violation of privacy and privilege information. Nonetheless, there shall be no violation of privacy if the investigator or authorized officer access the computer according to s 249 of the Communications and Multimedia Act 1998 (CMA) and s 79 of the Digital Signature Act 1997 (DSA) which provide that the data stored in the computer or otherwise can also be accessed by the police officer or the authorised officer. Similarly, s 10 of the Computer Crimes Act 1997 (CCA) also confers powers of search, seizure and arrest to any police officer. However, both CMA and DSA require the officers, the police officers and the authorised officers to obtain written consent from the Minister of Energy, Water and Communications prior to conducting a search and seizure.

Development of New Technology and New Crimes

Forensic analysis must present accurate result to the court. In order to do so the computer forensic expert must have good skills and knowledge on the computer forensic and also digital forensic science. Their findings will be considered by the court as expert opinion and their role is recognized not only in Malaysia but also other countries. The admissibility of computer forensic evidence is not specifically stated in the Evidence Act 1950 but section 45(1) of the Act recognizes the opinion of persons especially skilled in science. Their opinions are considered as relevant facts. The expert must also follow certain procedures when giving evidence. However, what may challenge the computer forensic investigators or experts is on the new technology, new technique and new tools used by the criminals to commit crimes in cyber space such as cloud computing, which is difficult as it is multi-tenant hosting, synchronization problems and techniques for segregating the data in the logs. Hence, in order to tackle these challenges, the investigator and forensic expert need to use and apply appropriate searching mechanism such as using abstraction layers, correct digital forensic analysis tools and be prepared to adopt new techniques to search for the computer data or digital evidence. Knowledge of digital forensic is dynamic and changing with times and thus it is necessary for IOs to be updated of any new technology probably being used by the criminals.

Proving the Reliability, Authenticity and Accuracy of computer evidence

Procedurally, criminal cases must be proved beyond any reasonable doubt while civil cases require the counsels to prove such cases on the balance of probabilities. Usually, proving the reliability, authenticity and accuracy of computer evidence may involve civil and criminal cases. Hence, it is not an easy task to do so since documents in electronic format have a number of features and available at various places. Since, the court accept only relevant documents which the Evidence Act 1950 has laid down under several provisions on the need to produce relevant documents. They are sections 6, 35 to 38 and sections 90A to 90C. The court will also accept admissions and witness statements to prove the authenticity of the evidence. Thus, the witness must be able to identify the evidence and explain in court. The insertion of sections 90A, 90B and 90C to the EA 1950 affirm that evidence from computer is admissible if produced in compliance with the stated EA 1950 provisions.

Multiple Jurisdictions

The borderless nature of the internet has allowed the commission of crimes from anywhere around the world. Since internet is one of the sources of computer evidence determining the law governing such evidence is sometimes very challenging. The challenge is to gather the evidence, investigate and prosecute the suspect who is living in other country but committing the offence in Malaysia. In this situation, working with INTERPOL is one of the best ways to arrest the suspect. However, if the evidence is not sufficient the suspect may escape from any liability. In Malaysia, problem on cross border issue can be referred to provisions under the CPC (section 127A which provides on liability for offences committed out of Malaysia); Extra-territorial Offences Act 1976; Computer Crimes Act 1997 (CCA) (section 9 which provides that, „ the Act shall apply to any person who have committed an offence outside Malaysia“.) and the Mutual Assistance in Criminal Matters Act 2002 (MACMA). Under these statutes the suspect will still be liable as if he has committed the crimes in Malaysia.

The Law May Be Outdated and Reliance Will Be on The Case Law

The technology develops very fast but the law needs times for review and updated. Nonetheless, this does not mean there must be a new law for every new technology. Traditional law can still be used but with some modifications and updated. In Malaysia, although there are several cyberlaws, only few laws are referred too when there are cases of hacking and misuse of network facilities, The relevant laws are the Computer Crimes Act 1997 (CCA) and the Communications and Multimedia Act 1998 (CMA). The hacking attacks in June 2011 on almost 200 websites by "Anonymous" hackers' group had given impact to the way issues on how cyber-attacks were handled. The Government has tightened the level of security in this country while the public are more aware of the attacks. Although these attackers will continue to find new ways to launch the cyber-attacks, the challenges can be handled if the enforcement of the existing laws (particularly the cyberlaws) is improved. In view of this, the Malaysian Government has introduced a new law called the Cyber Security Act 2024.

Cyber Security Act 2024

The Cyber Security Act 2024 has been officially gazette by the Attorney General's Chambers on 26 June 2024. This legislation is a major milestone in strengthening Malaysia's cyber defenses and enhancing our resilience against emerging threats (NACSA, 2024).

The Cyber Security Act 2024 introduces several important features, such as the establishment of the National Cyber Security Committee. It outlines the duties and powers of the Chief Executive of NACSA (National Cyber Security Agency), as well as the functions and duties of the National Critical Information Infrastructure (NCII) sector leads and NCII entities. The act also addresses the management of cyber security threats and incidents related to NCII. Additionally, it includes provisions to regulate cyber security service providers through licensing.

In exercise of the powers conferred by subsection 1(2) of the Cyber Security Act 2024 [Act 854], the Prime Minister appoints 26 August 2024 as the date on which the Act comes into operation.

NACSA is dedicated to ensuring the effective implementation of this Act, which will have a vital role in protecting our digital environment and earning the trust of all Malaysians.

Artificial Intelligence (AI) and Criminal Investigations

Integrating artificial intelligence (AI) into criminal investigations can expedite the process, generate high-quality evidence, and enhance law enforcement efforts. However, like any technological advancement, it raises significant ethical questions and potential for misuse (Lunter, 2023).

AI applications in criminal investigations offer several promising advancements which include among others:

1. AI-Driven Fingerprint Analysis: AI can rapidly identify latent fingerprints, significantly reducing the time compared to manual forensic methods. However, the accuracy of these identifications still needs to be verified by trained forensic experts, ensuring that AI serves as a supportive tool rather than a decision-maker (Lunter, 2023)

2. Criminal and Victim Data Analysis: AI is revolutionizing the analysis of criminal justice data by predicting recidivism and improving warrant management. Researchers at the Research Triangle Institute, with support from NIJ, are developing a triage tool for North Carolina's Statewide Warrant Repository. By analyzing over 340,000 warrant records, their algorithms can forecast when a warrant might remain unserved, assess the risk of re-offending, and optimize resource allocation by targeting high-risk areas (Taniguchi et al., 2019).

While these aspects of AI being integrated into criminal investigations in countries like the US and the UK, Malaysia is still in the process of drafting bill to enact a legislation that includes AI governance and ethics code that guarantee accountability and transparency, and ccontrolling of cyber security risk.

AI Regulations in Other Countries

The use of artificial intelligence (AI) in criminal investigations varies significantly across different countries and legal frameworks. In the United States, AI technologies are extensively employed in predictive policing and facial recognition. One notable example is the use of predictive policing tools such as PredPol, which analyzes historical crime data to anticipate potential future crime hotspots. Additionally, facial recognition technology has been employed by law enforcement agencies such as the FBI to identify suspects from surveillance footage (Lau, 2020; Epstein & Emerson, 2024).

In the United Kingdom, AI technologies have been employed for crime analysis, crime prediction and investigative purposes. For instance, ssome police forces across the UK which include the Metropolitan Police Service in London have uutilized AI to analyze large volumes of data to predict and prevent crimes (Mahalias, 2024).

In Australia, the Australian Federal Police (AFP) utilizes AI for cybersecurity investigations and improving the analysis of digital evidence. The AFP has stated that it engages AI to examine data collected through telecommunications and surveillance warrants, with a commitment to maintaining full transparency regarding the technology's use (Taylor, 2023).

Malaysia, similar to numerous other nations, finds itself at a critical juncture in the progress of AI, carefully managing the interplay between scientific breakthroughs and the legal, ethical, and sociological consequences. Firstly, the analysis has revealed that Malaysia's current legal framework has some deficiencies and uncertainties about AI-related matters such as liability, accountability, data privacy, intellectual property rights, and algorithmic transparency. The presence of these gaps introduces uncertainty and potential hazards for the stakeholders engaged in the development, implementation, and utilization of AI.

Hence, it is imperative to revise and strengthen Malaysia's legal framework to tackle the distinct difficulties presented by AI technology. Furthermore, it is crucial to emphasize the importance of implementing a proactive regulatory framework.

CONCLUSION

The advancement in technology can change the method of collecting and proving computer evidence. The laws should be able to cope with the technological changes. In future, there may be more complicated cases and tracing the electronic or computer evidence will be more challenging. Inadequacy in laws and criminal investigation procedures might provide opportunity for the suspect to escape from any liability. Hence, setting up a precedent from cases is very important in order to provide a good reference for future cases. At the same time, there must also be continuous efforts to update and amend the laws and regulations with regard to criminal investigation process in the context of technological advancement particularly, in the use of Artificial Intelligence where criminals have increasingly become technology savvy.

As society relies more on computers and the internet for financial transactions, the convenience of monitoring our financial activity is paired by the rising risk of cyber-deception and theft. Technological devices and specialized software are turning into essential tools in the fight against the growing wave of cybercrimes, which highlights the significance of a complex legal system. The study emphasizes how new and developing technologies are revolutionizing criminal justice and crime prevention, underscoring the necessity for flexible legal frameworks that strike a balance between the growth of technology and the defense of civil liberties and the effectiveness of law enforcement.

To navigate these challenges effectively, it is essential to update legal frameworks to account for technological advancements, focusing on privacy laws and bias mitigation. IOs in Malaysia need to be ready in facing these new challenges. In fact. ffuture studies need to explore more detailed aspects of the impact of emerging technologies within specific countries or analyzing particular legal systems. This would allow legal researchers to address gaps and develop a more nuanced understanding of how various jurisdictions adapt to technological advancements in criminal investigations. This paper offers insightful information to scholars, legal experts, and

legislators who are attempting to understand how law and technology are interacting in the digital age.

REFERENCES

1. Anita Harun, Ramalingam Rajamanickam & Insyirah Mohamad Noh (2022). Admissibility Of Electronic Evidence in Malaysia, Baltic Journal of Law & Politics 15:7 (2022): 1352-1360
2. Durayana Mohamed. (2011). Computer evidence: Issues and challenges in Present and in the Future, 6th UUM International Law Conference (ILC) 2011.
3. Durayana Mohamed & Zulfikar Ramlee (2014). Cases of electronic evidence in Malaysian courts: The Civil and Syariah Perspective. ICSSR e-Journal of Social Science Research. Vol 1 No 2 2014, pp. 1-10
4. Epstein, B., & Emerson, J. (2024). Navigating the Future of Policing: Artificial Intelligence (AI) Use, Pitfalls, and Considerations for Executives. Police Chief Online. Retrieved Online from
5. Lau, T. (2020). Predictive Policing Explained. Brennan Center for Justice. Retrieved Online from
6. Lunter, J. (2023). Can criminal investigations rely on AI? Retrieved from
7. Mahalias, I. (2024). AI adoption in criminal justice – How can industry support the justice system in implementing Artificial Intelligence. Retrieved Online from criminal-justice-how-can-industry support-the-justice-system-in implementing-artificialintelligence.html.
8. NACSA, Cyber Security Act 2024. Retrieved Online from
9. Nurul Syazwani Abdullah Kahar, Wan Abdul Fatah Wan Ismail, Ahmad Syukran Baharuddin & Lukman Abdul Mutalib (2021). The Admissibility of Digital Document as Evidence Under Malaysian Civil Court. Proceeding of the 8th International Conference on Management and Muamalah 2021 (ICoMM 2021) e-ISSN: 2756-8938
10. Radhakrisna, G. (2016). Section 90A of Evidence Act 1950 of Malaysia: Time for Review Proceedings at the 5th Annual International Conference on Law Regulation and Public Policies
11. Radhakrishna, G, Myint Zan & Khong Wye Keen (2013). Computer Evidence in Malaysia: Where are We? Malayan Law Journal Articles/2013/Volume 3/ [2013] 3 MLJ xxxiii
12. Taylor, J. (2023). Australian federal police using AI to analyses data obtained under surveillance warrants. The Guardian. Retrieved Online from
13. Zainal Amin Ayub, Mohamad Fateh Labanieh & Harlida Abdul Wahab (2023). A Legislative Analysis of Malaysian Legal System on Search and Seizure Procedure of Digital Evidence. R. Abdul Rahman et al. (eds.), Proceedings of the 12th UUM International Legal Conference 2023 (UUMILC 2023), Atlantis Highlights in Social Sciences, Education and Humanities 15,

Cases

1. Approfit Sdn. Bhd. v Kent Sing Construction Sdn. Bhd. & Ors [2001] 6 MLRH 749
2. PP v Ong Cheng Heong [1998] 4 CLJ 209
3. PP v Hanafi Mat Hassan [2003] 6 CLJ 459
4. Hanafi bin Mat Hassan v PP [2006] 4 MLJ 134
5. Gnansegaran a/l Pararajasingam v PP [1997] 3 MLJ 1
6. Bank Pembangunan Malaysia Bhd v. Sasacom Sdn Bhd & Another Case [2010] 1 LNS 1423; [2011] 10 CLJ 51
7. Avnet Azure Sdn Bhd v Eact Technologies Sdn Bhd and Sapura Research Sdn Bhd. KL HC Com. Div. D-22NCC439-2011.
8. Microsoft Corporation v Conquest Computer Centre Sdn Bhd. [2015] 7 MLJ 243
9. Standard Chartered v Mukah Singh [1996] 3 MLJ 240
10. Chua Boon Hong v PP [2011] MLJU 1332, [2011] 1 LNS 1773 CA.
11. Schmidt Scientific Sdn Bhd v Ong Han Suan [1997] 5 MLJ 632

Statutes

1. Evidence Act 1950
2. Computer Crimes Act 1997 (CCA 1997)
3. Communications and Multimedia Act 1998
4. Cyber Security Act 2024