Volume 8. Nomor 2. Juli 2013

Pandecta

http://journal.unnes.ac.id/nju/index.php/pandecta

Evolution of Malaysian Cyber Laws and Mechanism for Secured Online Transactions

Yusuf Ibrahim Arowosaiye✉

Department of Public Law, Faculty of Law, University of Ilorin, Nigeria

Info Artikel

Sejarah Artikel:
Diterima April 2013
Disetujui Mei 2013
Dipublikasikan Juli 2013

Keywords:
Malaysian Cyber Law; online transaction; information technology

Abstrak

Penelitian ini dimaksudkan untuk mendeskripsikan tentang kerangka hukum pengaturan hukum siber dan mekanisme pengamanan transaksi online di Malaysia. Pendekatan analisis adalah perundang-undangan mengenai konsep perlindungan dan proteksi transaksi online. Secara komprehensif pembahasan dilakukan dengan melihat secara historis perjalanan hukum siber di Malaysia sampai pada perkembangan mutakhir. Hasil kajian ini menunjukkan bahwa kemajuan sistem hukum siber Malaysia diarahkan untuk mendukung Visi global 2020 untuk menjadikan Malaysia sebagai salah satu kekuatan dunia dalam kemajuan teknologi informasi, sehingga berbagai produk hukum dibidang teknologi informasi diarahkan menuju tercapainya visi tersebut.

✉Alamat korespondensi:
P.M.B. 1515, Ilorin, Kwara State, Nigeria
E-mail: ibrahimyusuff@gmail.com

ISSN 1907-8919 (cetak)
ISSN 2337-5418 (online)

1. Introduction

"Information Technology has taken the worlds by storm. Men are left with two options, either to accept and take advantage of it or shun it and be left in wilderness. The former option if chosen could bring mankind into light of knowledge unimaginable; whereas the latter option can lead to retrogression and darkness. It is for this reason that the Malaysian Government has taken the first option, thus marking the beginning of a new era of knowledge based society….. ".
(Dr Mahathir bin Mohamad, Former Prime Minister, Malaysia.Kuala Lumpur, 11th June, 1999).

The development of information technology law in Malaysia can be attributed to the Malaysian national ambition to become a truly developed nation by the year 2020. To achieve this lofty goal, the Malaysian government emphasised the importance of information and communication technology especially its application in the socio-economic life of the Malaysian people (Hamin, 2004:210-33). Therefore the major push in the Malaysian national developmental plan is to build a "knowledge-based economy". To actualise this vision, a National IT Agenda (NITA) was formulated which comprises of a combination of goals and means as to roles of information, knowledge and entrepreneurship working together to transform the Malaysian economy into a "knowledge economy" and the Malaysian society into a "knowledge oriented society" (Hamin, 2004:2010-33; Tipto, 2002:83-99).

In line with the above national ambition, Malaysia embarked on a Multimedia Super Corridor (MSC) project which is a major national initiative designed to satisfy the

country's ambition of assuming the status of a developed nation by the year 2020. To make the Multimedia Super Corridor (MSC) project more pragmatic and concrete in implementation, seven primary areas of multimedia applications were identified.[1] These "flagship applications" offer an enormous opportunity to local as well the international business community through the provision of concessions and guarantees. The flagship applications are facilitated by respective government ministries who work directly with both local and international multimedia companies on the idea of the concept and implementation plans (Tipto. F. 2002; Ariff and Chuan. 1998:58).[2]

It is obvious therefore that to develop Malaysia as an advanced IT based society, a parallel development in information technology law is imperative. In line with this, the Malaysian government took the right first step by enacting a set of cyber laws, six in total, to actualise its national plan. These cyber laws are; Digital Signature Act 1997, Communication & Multimedia Act 1998, Computer Crimes Act 1997, Telemedicine Act 2000, Optical Discs Act 2000 and the amendment to the Malaysian Copyright Act of 1987.

Against the above backdrop, this discourse focuses on the development of information technology law in Malaysia. The paper also examines the relevant cyber laws put in place to engender secure and safe online transactions in Malaysia. Suggestions are also proffered on the aspect of the Malaysian cyber laws put in place to promote safe and secure online transactions.

1 The seven flagship applications areas with the lead governmental agency are Electronic Governance (lead agency : Malaysian Administrative Modernisation & Planning Unit (MAMPU)), MultiPurpose Card (Lead agency : Bank Negara (Central Bank of Malaysia)), Smart School (Lead agency : Ministry of Education), Telemedicine (Lead agency : Ministry of Health), Worldwide Manufacturing Webs (Lead Agency: Ministry of Int. Trade & Industry), R&D Clauster(Lead agency : Ministry of Science, Tech & Environment), and Borderless Marketing (Lead agency: Multimedia Dev. Corporation (MDC)).

2 Ibid . See also Ibrahim Ariff and Goh Chen Chuan. 1998. Multimedia Super Corridor. Leeds Publications. 58.

2. The Evolution of Information Technology Law in Malaysia

With advancement in information communication technology, different forms of digital technologies have emerged which have the potential to improve our socio-economic cum political lives and make business more efficient. Within a few years of this development, information technology permeated every aspect of day-to-day living such that one can hardly complete his daily activities without interaction with digital technology. This advancement has indeed made information more accessible, transactions faster and communication easier than what could be imagined in the last century. Indeed it can be asserted without any fear of contradiction that the entire human civilisation has been completely transformed by the technological advancement or digital revolution of the late 20th century. Malaysian survival of the Asia economic crisis in the 1980s was followed by rapid economic growth and development in her infrastructures in the early to mid 1990s. The resolve to move to the next level of development is consolidated by creation of a vision of modern Malaysia which is known as Malaysian Vision 2020 (Wawasan 2020; John, K.K.2001).

The objective of the Malaysian Vision 2020 is to place Malaysia in the position of an economically developed and industrialised nation by the year 2020. As a follow up to this national developmental plan, the Malaysian government came up with a plan for the creation of Multimedia Super Corridor (MSC), a 15 km by 50 km corridor which was to be the centre of information development in Malaysia.[3] The expectation of the Malaysian government with the MSC project is that it should attract the best and most successful multinational cooperation and institutions in the IT industry to set up and participate in developing the IT industry in Malaysia.

The success story of MSC today can be attributed to the commitment of

3 The MSC project is a designated area of 750 square kilometre of high technology zone from Kuala Lumpur City Centre to the KL International Airport .

the government of Malaysia in taking the initiative to put in place the appropriate information technology laws or cyber laws. The participation of IT giants like Microsoft, Oracle and Silicon Graphics was a boost to the realisation of the MSC project. These corporations were expected to establish research and development (R&D) facilities and make the MSC a hub for "software solutions", and to contribute tremendously to the success of MSC project. The MSC project was also designed to attract foreign investors, thus the project relies on both "hard" IT infrastructure and "soft" infrastructure (Halim, (no.year). The reliance on "hard" IT infrastructure by the project is to develop a modern high-speed telecommunication media links between all businesses, government offices, homes and as a modem for direct link to the rest of the world. The "software" infrastructure on the other hand is "concerned with business and investor-friendly incentives including tax exemption between five to ten years, unrestricted employment of knowledgeable workers and non-censorship of internet" contents (Hamin, 2004: 2, 211; Abdullah. 1996:26-27).

With the above IT developmental plan and design, it became obvious that necessary legal framework must follow suit if the Malaysian national plan through the IT project must be realisable. In respect of "software" infrastructure, two sets of information technology laws are necessary; "commerce enabling cyber laws and societal cyber laws" (Hamin, 2004: 2, 211; Abdullah. 1996:26-27). As for commerce enabling information technology law, the Digital Signature Act of 1997 which governs electronic signatures was enacted and the Copyright (Amendment) Act of 1997 was also enacted to enhance intellectual property protection and the Multimedia Convergence Act also of 1997 was also enacted to streamline communication, information and broadcasting services.

However, in the case of societal information technology laws, the Computer Crimes Act of 1997 was enacted to regulate the criminal use of computers and the internet. The Computer Crimes Act of 1997 criminalises unauthorised access to and modification of computer contents. An enactment in relation to health care is the Telemedicine Act of 1997. The Telemedicine Act of 1997 engenders a delivery of high quality healthcare services to the entire population regardless of their status and location through virtual medical consultation (Kassim. 2008).[4] Thus, the above enactments were introduced to assure investors of the seriousness of the government in protecting their investments through adequate legal and policy framework. Against the above backdrop, the rest of this discourse shall be devoted to the existing Malaysian information technology laws or enactments.

However, this discourse shall examine, in view of these existing Malaysian cyber laws, the approach taken by the Malaysian government to promote safe and secure online transactions in Malaysia.

3. The Malaysian Information Technology Laws

As earlier noted in this discourse, six primary cyber laws or information technology laws were enacted in response to the need of the Malaysian Multimedia Super Corridor (MSC) and the Malaysian national ambition to become a developed nation by the year 2020. These cyber laws are;

a. Copyright (Amendment) Act 1997

The advancement recorded in global information technology most especially the expansion and availability of copyright materials in the digital network has led to the polemic debate on the proper policy on information and knowledge based products in the new media (Azmi. 2002:13-40). The debate sprouts from the amazing potentiality of digital network in enabling infringement of

4 The Development E-medicine in Malaysia and Ethical Implications. (Unpublished Article), Accepted for publication in the next edition International Medical Journal. Note that the Malaysian E-medicine is designed to enhance citizen's equality in the availability of various medical services and clinical healthcare despite economic and geographical barriers. It is also aimed to enable easier access to rural based population to gain regular access to quality medical care.

copyright easier than ever. This phenomenon however prompted the view that copyright is a dead wood in the digital network (Azmi. 2002:13-40; Barlow J.1994). The fear is anchored on the ease by which copyrighted works can be replicated and distributed to others via the internet. Thus enforcement of copyright is becoming a nightmare. In response to this digital reality and its downside in relation to copyright materials, the United States presented a strong case before the World Intellectual Property Organisation (WIPO) for a legal intervention. The forceful lobbying manifested in the conclusion of the WIPO Copyright Treaty of 1996 (Barlow J.1994).

Without going into the details of the content of WIPO Treaty of 1996, it is instructive to note that Malaysian Copyright Act of 1987 fell short of the expectations and challenges brought about by the development in the global information communication technology. Therefore with the MSC project, appropriate amendment was made to the Malaysian Copyright Act of 1987 to reflect and protect online and digital works (Barlow J.1994). Most commendably, the Malaysian government, in living up to its determination to transform the country into a knowledge-based society together with IT giants who are partners to the MSC project, wasted no time in incorporating the major proposal for amendment forwarded by WIPO Copyright Treaty of 1996 into the local copyright law even before the treaty was ratified by the Malaysian government. Thus, the new Malaysian Copyright (Amendment) Act 1997 which incorporated the WIPO Copyright Treaty of 1996 was introduced. The objective of the amendment stated lucidly in the explanatory note to the Act as follows:

"Technology development, especially technology, has challenged traditional concepts of copyright protection. The proposed establishment of the Multimedia Super Corridor (MSC) will generate both challenges and opportunities for Malaysians. The success of the MSC will, to a certain extent, be determined by the contents that move through it. These include educational works, entertainment products and information that are protected under copyright law. For the MSC to realise its full potential, it is essential that adequate legal protection be made available to these works. The Act is proposed to be amended towards this end, taking into account recent international developments in respect of certain copyright works."

In line with the above, the following are the major modes of copyright infringement added in the new amendment to the Malaysian Copyright (Amendment) Act 1997 (Sagal, P.S. 2001:89-124):

1. circumventing or causing the circumvention of any effective technological measures that are used by authors in connection with the exercise of their rights and that restrict acts not authorised by them,
2. the removal or alteration of any electronic rights management information without authority , and
3. distributing, importing for distribution or communicating to the public, without authority, works or copies of works in respect of which electronic rights management information has been removed or altered without authority.[5]

b. Telemedicine Act 1997

The development of information technology under the Malaysian legal system is well encompassing. In other words, the digital integration is not limited to governance and economy but it also transcends to digitalization of educational system and health care delivery. The IT development in the field of health care system is known as "Telemedicine" or "e-medicine". The term e-medicine or telemedicine means the provision of medical information and services through the use of telecommunication or electronic or digital means. A statutory definition was given by Section 2 of the Malaysian Telemedicine Act 1997 to mean the practice of medicine using audio, visual and data communications.

Thus, by virtue of Section 3 of the Act, no

5 Among other changes introduced by the Malaysian Copyright (Amendment) Act 1997 are; the introduction of communication right, the clarification of the term "fixation", the introduction of prohibition of anti encryption devices.

person may practice telemedicine other than a fully registered medical practitioner holding a valid practicing certificate or registered or licensed outside Malaysia but must be issued telemedicine practicing certificate by the Malaysian Medical Council. It is important to stress here that the Malaysian Telemedicine Act 1997 as information technology law is enacted to safeguard online medical transactions or consultation and purchase of medical drugs so that such transactions will be safe and secure. To achieve this objective, Section 3 of the Malaysian Telemedicine Act of 1997 provides that any person who practices telemedicine in contravention of this law, notwithstanding that he so practices outside Malaysia, shall be guilty of an offence for which the penalty may be a maximum of RM 500,000 or imprisonment for a maximum of five years or both.

It is hereby submitted that the above provisions are apposite in view of IT development taking place in Malaysia and it is expected that when e-medicine finally takes-off, more online medical consultation, sale and purchase of medical drugs would be experienced. All these will involve online services and transactions. It was recently disclosed by Medical Online Sdn Bhd, the developer of the Multimedia Super Corridor (MSC) flagship application in telemedicine that medical experts are to earn RM400 million to RM500 million in revenue during its five years concession period. This huge revenue will be generated through the sale of the application overseas and by licensing the software to end users for consultations or discussions (Star, 21 September : 1; Yuhai Tu. 2000: 353).

c. Communications and Multimedia Act 1998

The Malaysian Communications Multimedia Act 1998 was enacted to provide the policy and regulatory framework for the convergence of the telecommunications, broadcasting and internet industries. In line with the Malaysian IT national plan, Communications Multimedia Act 1998 repealed the Telecommunications Act of 1950 and the Broadcasting Act of 1988. The activities and services regulated under this Act include traditional broadcasting, telecommunications and online services.

To safeguard and secure online transaction, Part X (Chapter 2 Additional Offences and Penalties), Sections 231 and 241 of the Communications Multimedia Act 1998 enumerated some offences which are relevant for the purpose of e-commerce or online transactions in Malaysia. Thus, Section 231 of the Act provides that it is a criminal offence for any person to use any apparatus or device, without authority, with intent to obtain information regarding the contents, sender or addressee of any communication. To further secure online communication transaction, the Act declares under Section 232 that it is an offence for a person to fraudulently use network facilities, network services, e.t.c.; improper use of network facilities is also an offence under Section 233 of the Act. Aside from the above online communication offences, the following are also declared as an offence under the Act (Sagal, P.S. 2001:16, 97):

1. Section 234: Interception and disclosure of communications without lawful authority
2. Section 235: Damages to network facilities
3. Section 236: Fraud and related activities in connection with access devices
4. Section 239: Unlawful use, possession or supply of non standard equipment or device and
5. Section 240: Distribution or advertising any communication equipment or device for interception of communication.

d. Malaysian Communications and Multimedia Commission Act 1998

The Malaysian Communications and Multimedia Commission Act 1998 was among the first set of information technology laws to be passed in 1998 and it came into force the same year. The statutory function of this Commission is to supervise and regulate communications and multimedia activities in Malaysia and to enforce the relevant laws (Surin, A.J.2006:1). The role of the Commission is very crucial which is

to implement and promote the national objectives of the Malaysian government for the communication and multimedia sector. The commission is also the certifying agency under the Digital Signature Act of 1997 (Surin, A.J.2006:1). Since the Commission implements and enforces the provisions of the Malaysian Communications Multimedia Act 1998, it is expected to play a major role in regulating e-commerce in Malaysia.

e. Digital Signature Act 1997

The development of the Malaysian information technology law could not be complete without the enactment of the Digital Signature Act of 1997. The reason being that the advancement in information technology and its integration in almost all aspects of human endeavours, especially commerce and trade, creates a situation whereby computer and other ICT infrastructures are being used to create, transmit and store information in electronic form. Traditional paper documentation is vastly becoming unpopular and less attractive since electronic storage of information is cheaper, easier to store, retrieve and can be transmitted with amazing speed.

The traditional paper based records and documentation as well as signatures appearing on physical paper are well recognised under most legal provisions that are yet to respond to digital documentation. The reality of online transactions or electronic commerce presents a situation which eliminates the traditional methods and requirements associated with paper transactions. Thus the need for given legal recognition to electronic signatures and digital signatures becomes pertinent if Malaysia truly aspires to be a technology based society. The above reality leads to the enactment of the Malaysian Digital Signature Act of 1997 which came into force on October 1, 1998 together with the Digital Signatures Regulations of 1998 (Sagal, P.S. 2001, n. 16, p. 99).

The primary objective of Digital Signature Act of 1997 is to encourage electronic transactions, especially commercial transactions and to curb forgeries and computer generated frauds. It is instructive to stress that the State of Utah became the first state in the United States to enact digital signature legislation sometime in 1995 (Munir, 1999:186). It is also remarkable that Malaysia is among the first countries, outside U.S.A., to follow the State of Utah. The enactment of the Digital Signature Act of 1997 is rightly considered to be imperative legal framework to thrust the digital technology that will further revolutionise electronic commerce in the world and Malaysia in particular by providing a more secure means of online transaction and identification procedures (Munir, 1999:186; Closen and Richard, 1997:733). Section 64(1) of the Digital Signature Act of 1997 provides that;

"A message shall be as valid, enforceable and effective as if it had been written on paper if- *(a)* it bears in its entirety a digital signature; and *(b)* that digital signature is verified by the public key listed in a certificate which- (i) was issued by a licensed certification authority; and (ii) was valid at the time the digital signature was created.

By the above provision, a digitally signed message is deemed to be a written document (Closen and Richard, 1997:733). Thus, while the Digital Signature Act of 1997 provides for and regulates the use of digital signature, it fails to provide for matters relating to electronic contract (Sagal, P.S. 2001, n. 16, p. 100). The legal implication here is that while the Malaysian Digital Signature Act of 1997 fails to expressly govern e-contract or commerce, such contract will be governed under the old Contract Act of 1950. It is obvious that the Contract Act of 1950 did not envisage regulation of digital forms of contract at the time it was enacted and therefore is not in a position to adequately cover e-contract (Sagal, P.S. 2001, n. 16, p. 100). Be that as it may, it is hereby recommended that the Contract Act of 1950 be amended to reflect the need for digital or e-contract. This is necessary against the fact that other similar jurisdictions like Singapore and India have enacted Electronic Transaction Act of 1998 and Information Technology Act of 2000 respectively (Sagal, P.S. 2001, n. 16, p. 100).

Since our preoccupation in this discourse is the development of Malaysian

information technology and measures put in place to ensure safe online transactions, it is imperative to examine the purpose of the Digital Signature Act of 1997 in achieving this objective. A comprehensive caption of the objectives of the Malaysian Digital Signature Act of 1997 can be better gleaned from the similar purpose for which the State of Utah's Digital Signature Act (UDSA) was enacted being the first of its kind and a model for many other states in U.S.A, and many other countries in the world. The common objectives of the Malaysian Digital Signature Act of 1997 as well as the Utah Digital Signature Act of 1995 are as follows (Munir, 1999. n. 22, 189);

1. to minimise the incidence of forged digital signatures and enable the reliable authentication of computer based information;
2. to enable and foster the verification of digital signatures on computer- based documents;
3. to enable commerce by means of computerised communications'
4. and to give legal effect to certain technical standards.

The above objectives of the Malaysian Digital Signature Act of 1997 speaks volumes of the development of information technology law in Malaysia and the legislative protections inbuilt in the Malaysian cyber laws to promote safe and secure online transactions. The above definitely are the substantive legal framework. On the practical and procedural aspects; the Malaysian statute designates hree primary players in the digital signature certification process: the subscribers, (Munir, 1999. n. 22, 189)[6] the recipient,[7] and the certification authority.[8]

The recipients are the receiver of the documents who access those documents through their public keys. Certification authorities issue the certificates that verify the digital signatures. Furthermore, the Act allows the establishment of licensed certification authorities, who may issue certificates identifying a particular subscriber (Section 2 of the Malaysian Digital Signature Act 1997). The law however requires that digital signature verification be accomplished by the process of encryption (Section 2 of the Malaysian Digital Signature Act 1997).

In order to make the process of digital signature more secure and reliable for online transactions in Malaysia, Part II of the Malaysian Digital Signature Act 1997 provides for the appointment of a Controller of Authentication Authorities by the Minister for the purpose of monitoring and overseeing the activities of certification authorities (Section 321 of the Malaysian Digital Signature Act 1997). Further more, it is a criminal offence that attracts punishment to operate as a certification authority without a valid licence.[9]

In view of the above provisions and practical measures accompanying the Malaysian Digital Signature Act 1997, the pertinent question to ask here in view of the subject of this discourse is 'how safe is the digital certificate in relation to online transaction in Malaysia?' In view of the reasonable fear of insecurity of the digital signature in Malaysia against theft, tampering and unauthorised use and most importantly the protection of the primary subscribers, this is taken care of in the regulations under the Malaysian Digital Signature Act 1997. More specifically, Part IV, entitled, "Suitable Guarantees and Claims", of the Digital Signature Regulations 1998 provides suitable guarantees against these anticipated problems.

However, the following have been identified as the common deficiencies in the Malaysian Digital Signature Act 1997 in ensuring safe and secure online transactions (Munir, 1999. n. 23, 190- 191);

6 Section 2 of the Malaysian Digital Signature Act 1997 defines a subscriber as a person who: (a) is the subject listed in a certificate; (b) accepts the certificate; (c) holds a private key which corresponds to public key listed in that certificate.

7 Section 2 of the Malaysian Digital Signature Act 1997 defines a recipient to mean a person who receives or has a digital signature and is in a position to rely on it.

8 Certification authority under Section 2 of the Act means a party or person who issues a certificate.

9 See Section 4 (2) of the Malaysian Digital Signature Act 1997. The punishment for operating as certification authority without a valid licence on conviction, is a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding ten years or both.

1. an individual subscriber to digital signature is obligated not to allow his private key to fall into the hand of someone else since such neglect means acceptance of damages resulting thereof where documents signed with the key, e.g. to demand for the withdrawer of money from his bank account even without approval by the subscriber;
2. the public cryptography does not reduce the risk involved in the signing of an electronic document but rather transfer such risk completely to private key,
3. that the Act though transfer the risk to the subscribers, they are only require to exercise reasonable duty of care in retaining control of the private key. That this standard id insufficient as absolute duty to retain exclusive control of the private key will increase the integrity and confidence in digital signature and create more precaution in keeping private key;
4. that the law allow only the use of the "asymmetric cryptosystem" to verify digital signatures. This restriction to one methodology may serve to hamper rather than promote the systematic use of advance and more secured signature technologies in the future.
5. the Malaysian Digital Signature Act 1997 did not set any standard for or any qualification for the certification authorities,
6. the intention of the law makers in respect of guarantees is to limit the liabilities of the certification authorities through the "recommended reliance limit", the Act do not set any specific amount required a bound; Another downside of the law on subscribers is that the certification authority has access to transaction information and some of the information may be commercially sensitive.

f. Computer Crimes Act 1997

Malaysian government is resolute in its readiness to establish a knowledge based society facilitated by information technology (Harris and Faculty of Information Technology, University Malaysia Sarawak, 2010). The introduction of the MSC project necessitated the enactment of the six set of cyber laws as earlier mentioned. The tremendous opportunity provided by the internet to cyber criminals cannot be easily set aside in view of the inherent loopholes in the existing Malaysian penal enactment in dealing with computer or electronic related offences.

The Malaysian Computer Crimes Act 1997 was enacted as a response to the contemporary use of information technology to commit crime and to strengthen the prevention of misuse of computers. The Act is modelled on the UK Computer Misuse Act of 1990 with some minor modifications. Although the primary focus of the Malaysian Computer Crimes Act 1997 is criminalising hacking activities and its negative impact on socio-economic and political life of Malaysia, its other wider objectives cannot be denied. Aside from hacking, computer and internet can be used to commit other traditional offline crimes such as money laundering, advance fee fraud, forgery, piracy, drug dealing, tax evasion, gambling, extortion, prostitution to mention but a few. The scope of cyber crime is unimaginable.

Computer hacking no doubt is a real threat to the development of online transactions in Malaysia. The most ubiquitous methodology usually employed in computer hacking is by gaining unlawful access to computer systems or online materials with or without the primary intention to commit further offences (Bainbridg, 2000.307,310). Most often than not, the intention of computer hackers is to modify or erase the information or data kept in the computer system for the fun of it or to commit computer fraud (Jalil, 2002:155-177). This form of online criminal activity constitutes a serious threat to e-commerce and other online activities. It is most agonising to see companies or enterprises spending millions of dollars on system security or to investigate online crimes with the primary purpose of forestalling future occurrences which is not even guaranteed.

Against the above background, the Malaysian Computer Crimes Act 1997 classified the following acts in relation to computers and online transactions as

offences and prescribes penalties thus (Sagal, 2001. P.S. 2001, n.16, 92.;

1. Knowingly causing a computer to perform any function with the intent of securing unauthorised access to any program or data held in the computer. The penalty is a maximum of RM 50,000 or imprisonment for maximum of five years or both (Section 3 Malaysian Computer Crimes Act 1997);
2. committing an offence referred to in Section 3 with the intent to commit an offence involving fraud of dishonesty or which causes injury as defined in the Penal Code or facilitating the commission of such an offence whether by himself or any other person. The penalty is a maximum of RM 150,000 or imprisonment for a maximum of 10 years or both (Section 4 Malaysian Computer Crimes Act 1997);
3. doing an act knowingly which will cause unauthorised modification of the contents of any computer. The penalty is a maximum of RM 100,000 or imprisonment for a maximum of 7 years or both. But if the act is done with the intention of causing injury as defined in the Penal Code, the penalty will be enhanced to a maximum of RM 150,000 or imprisonment for a maximum of 10 years or both (Section 5 Malaysian Computer Crimes Act 1997);
4. communication directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorised to communicate. The punishment is a maximum of RM 25,000 or imprisonment for a maximum of 3 years or both (Section 6 Malaysian Computer Crimes Act 1997).
5. a person who abets the commission of or who attempts to commit any offence under this Act, or who does any act preparatory to or in furtherance of the commission of any offence under this Act, shall be guilty of the offence and shall be liable to the punishment provided for the offence: provided that any term of imprisonment imposed shall not exceed one half of the maximum term provided for the offence (Section 7 Malaysian Computer Crimes Act 1997).

It is important to state here that the enactment of the Computer Crimes Act 1997 is quite a watershed in the development of information technology under the Malaysian legal system. The Act as it were provides protection to online transactions as well as protects the computer system itself against unlawful access and deliberate criminal intention to cause destruction to the system by the criminal activities of hackers and others alike. Recently there was a report of an attempted cyber or computer crime involving some banks in Malaysia (Shuan, 2010). In August 21, 2000, it was reported that computer criminals sent false email to Maybank customers and offered users of "Maybank 2 U online tools" that could download from a website at maybank2u. rvx.net. In the real sense the tools were programme files, one of which was a Trojan horse, a destructive program that appears as an application. This crime was detected based on early report and the website was taken down by the host. It was believed that the criminal attempt was in order to collect passwords from online users. The existence of the Act makes it possible to prosecute the offender if arrested.

4. Conclusion

The development of information technology law under the Malaysian legal system and the measures put in place by the government to ensure safe and secure online transactions was necessitated by the Malaysian Vision 2020 and the setting up of the Multimedia Super Corridor (MSC) which is to launch Malaysia as a global force in IT industry. The setting up of MSC is a crucial project that is expected to transform Malaysia to a knowledge based society and electronic driven economy.

However, the development of information technology that is expected to serve as a catalyst in the realisation of Malaysian Vision 2020 was backed up with necessary legal framework so that the project

is not exposed to abuse. To this end, Malaysia passed a comprehensive set of Acts in 1997 which can now be considered as Malaysia's cyber laws. The six Acts as examined above complement one another in ensuring safe and secure online transactions. The said set of Acts may have some inadequacies but the reality is that their existence is very crucial to the sustainability of online transactions in Malaysia.

Reference

Abdullah, O.Y. 1996. Malaysian Plan for Technology Change. Australian Accountant.

Ali, A.H. Towards Malaysia's Knowledge Empowerment in the 21st Century in Building Knowledge Society: Access, Empowerment and Governance, MIMOS. Also available at http://www.nite.org.my.

Ariff, I. and Chuan, G.C. 1998. *Multimedia Super Corridor*. Leeds Publications.

Barlow J. 1994. Selling Wine without Bottles: The Economy of Mind on the Global Net. http://www.eff.org/pub/intelllectual- property/idea-economy.article

David I. Bainbridge, Introduction to Computer Law, Pearson Education, England, 2000, 4th edition, 307, and 310.

Ida Madieha bdul Ghani Azmi. 2002. Digital Technology, Copyright and Education: The Malaysian Perspective. *IIUM Law Journal* 10 (1).

Jalil, Md. A. 2002. The Impact of Hacking and other Computer Related Offences on the Growth of Electronic Commerce. IIUM Journal 10 : 155 – 177.

John, K.K.. The Malaysian Growth with Equity (GEM) Story: Leaping to a K-Society. Paper presented at the Asian Development Bank 3rd Annual Meeting of Board of Governors, Hawaii, 7th May, 2001. Also available at http://www.nitc.org.my

Mahathir bin Mohamad, the former Prime Minister of Malaysia, in a book titled "Cyber Law: Policies and Challenges" by the author Abu Bakar Munir, (Malaysia: Butterworth Asia,19999).

Malaysia's Multimedia Super Corridor, An IFTP NG9.4 Position Paper, October, 1998 by Roger W. Harris and Faculty of Information Technology, University Malaysia Sarawak. See http://is2.lse.ac.uk/ifipwg94/pdfs/malaymsc.pdf. Accessed on 12th June, 2010.

Michael L. Closen and R. Jason Richard. 1997. Notaries Public- Lost in Cyberspace, Key Business Professionals of the Future. The John Marshall Journal of Computer & Information Law xv (4).

Munir, A.B. Cyber Law : Policies and Challenges, Butterworths Assia, 1999.

Puteri Nemie Jahn Kassim. 2008. The Development E-medicine in Malaysia and Ethical Implications. (Unpublished Article), Accepted for publication in the next edition International Medical Journal.

Sagal, P.S. 2001. Electronic Commerce Law in Malaysia. *Journal of Law and Information Science* 11(1).

Supt Lm Hong Shuan, White –Collar Crime in Malaysia, available at http://mpk.rmp.gov.my/jurnal/2005/whitecollarcrime.pdf. Accessed on 12th May, 2010.

Surin, A.J, Cyberlaw and its Implications, Pelanduk Publications, Selangor- Malaysia, 2006, 1.

Tipton. F. 2002. Bridging the Digital Divide in Southeast Asia: Pilot Agencies and the Policy Implementation in Thailand, Malaysia, Vietnam and the Philippines. *ASEAN Economic Bulletin*.

Yuhai Tu. 2000. How Robust is the Internet?. Nature 406 (6794) : 353.

Zaiton Hamin. 2004. The Legal Response Computer Misuse in Malaysia – The Computer Crimes Act 1997. *UiTM Law Review 2*.

Section 3 Malaysian Computer Crimes Act 1997

Section 4 Malaysian Computer Crimes Act 1997

Section 5 Malaysian Computer Crimes Act 1997

Section 6 Malaysian Computer Crimes Act 1997

Section 7 Malaysian Computer Crimes Act 1997