CYBER-LAWS IN THE NEW ECONOMY: THE CASE OF MALAYSIA

Mudiarasan Kuppusamy
School of Business
Monash University Malaysia
No. 2, Jalan Kolej, Bandar Sunway,
46150 Petaling Jaya Selangor
Tel: 603-56360600
Fax: 603-58804358
Email: mudiarasan.kuppusamy@buseco.monash.edu.my

Santhapparaj Solucis
Faculty of Management
Multimedia University Malaysia
Tel: 603-83125699
Email: santhapparaj@mmu.edu.my

ABSTRACT

Today, information and communication technologies (ICT) have become a critical factor to the growth, progress and prosperity of a country. New technologies are a fundamental part of the new economy. However, new technologies have also raised numerous legal issues, which fall within the ambit of newly evolving discipline of law - cyberlaws. Most developed countries have taken relevant measures to protect themselves in the information economy. But most developing countries are still lagging behind in this context. Nevertheless, Malaysia, a fast progressing developing country in the Asian region, established several cyberlaws in recent years. In this context, this paper seeks to highlight the state of cyberlaws in Malaysia and the challenges in implementing the laws. Further, this paper also highlights some of the related cyber crimes, which proliferates the need for cyber laws to be enacted in the first place.

1. INTRODUCTION

The rapid development of information communication and technology (ICT) has brought in cultural, economic, political and social transformation all over the world. At the macro level, ICT contributed to significant economic growth in most developed countries in the past two decades. OECD (2001) reported that ICT investment in some developed countries has contributed between 0.3 to 0.9 percentage points of growth in GDP per capita over the 1995 to 1999 period. Other empirical studies have also shown that ICT improves productivity and economic growth in the developed countries since mid 1990s (e.g. Brynjolfsson and Hitt, 1995; Colecchia and Schreyer, 2002).

At the micro level, the emergence of the Internet, electronic business and electronic government expanded the ability to have unprecedented access to information. For example, Gourova et al. (2001) argued that Internet plays important role in connecting the developing countries with the developed countries. Thus, Internet is deemed as an important facilitator for the developing countries in achieving economic growth in the new economy.

The above-mentioned examples show that rapid diffusion of ICT brings significant amount of benefits in a country. However, ICT has also created complex new challenges, among which is the issue of legislation. In the information age, varying sets of approaches are required for controlling, regulating and facilitating electronic communication and commerce development. To this end, issues such as the identification of legal entities in cyberspace, privacy protection and intellectual property need to be closely regulated. Hence, enactment of cyberlaw is important. However, Edappagath (2001) cautioned that cyberlaw needs to be enacted by first knowing the extent of cybercrimes and its implications in each country.

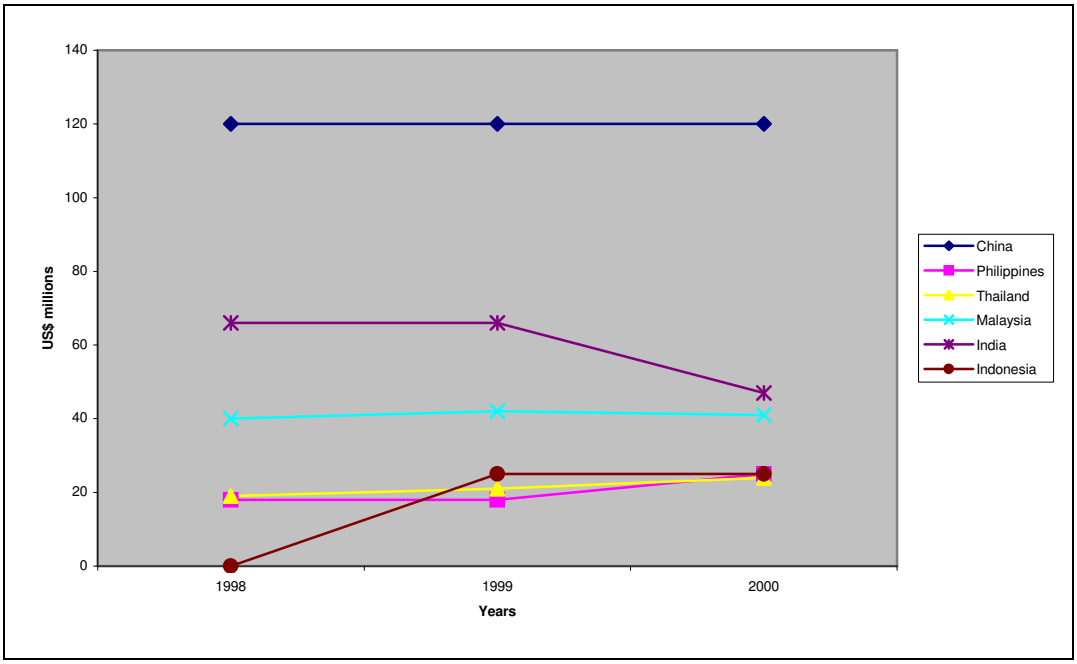
To the layman, the pertinent question often would be, what is cyberlaw? There are many definitions to the term cyberlaw. Edappagath (2001, p.2) provided the following definition to cyberlaw: *"the term cyberlaw in general refers to all the legal and regulatory aspects of Internet. It means that anything concerned with or related to activities of netizens and others in cyberspace comes within the ambit of cyberlaw"*.

In its simplest term, we define cyberlaw as the governing regulatory components of the ICT. One of the unique characteristics of cyberlaw is that it requires constant evolvement in tandem with technological development. In recent years, there has been a worldwide call for enactment of cyberlaws in order to justify the rapid increase in cyber crimes. For example, the Council of Europe's Convention on Cybercrime in 2001, promoted serious measures to counter cyber crimes and signed international treaty with US, Canada, Japan and 43 states of the Council of Europe taking part in the treaty. The Convention is among the first international treaty to address cyber crimes issue in depth (Council of Europe, 2001).

Albeit the international call for enactment of strategic cyberlaw, the developing countries are still in the dark on the issue of cyberlaw. Several reasons can be attributed to this. First, most developing countries are still newcomers in the information economy. The technological progress in these countries is still at infancy, thus there seem to be no

urgency for development of cyberlaw in the country. Nevertheless, some developing countries – Malaysia, India, China, Indonesia, Thailand and Philippines experienced consistent growth in ICT diffusion over the years. There is also considerable level of cyber crimes in these countries. Figure 1 shows the estimated level of copyright piracy trade losses in these countries over the period 1998 to 2000.

Figure 1: Estimated copyright piracy trade losses in US$ millions (1998-2000) in selected developing countries



Source: adapted from Urbas (2001)

Cyber crimes constitute one of the most important challenges facing cyberspace today. Cyber crimes refer to the activities done with criminal intent in the cyberspace or more specifically using the medium of Internet. These activities could be either criminal-based activity, socially motivated or politically instigated. In short, any activity, which offends human sensibilities, can be included within the ambit of cyber crimes. Cyber crimes exist in various forms – illegal telecommunication interceptions, electronic vandalism, theft of communications services, telecommunications and associated intellectual property piracy, electronic fraud, electronic funds transfer and money laundering (Grabosky and Smith, 1998).

Duggal (2001) highlighted that even though the numbers of cyber crimes have increased worldwide, most developing countries are not enacting appropriate legislation to cover them. The existing cyberlaws in the developing countries does not cover most of the cyber crimes. For example, in 2000, a hacker from the Philippines released the *'I Love You'* computer virus, which caused worldwide damages and losses amounting to billions of dollars. However, he could not be convicted due to non-availability of relevant cyberlaws in Philippines.

In recent years, security hacking activities are on the rise in Asia. The recent Bali bombing attack in 2002 has seen heightened cyber attacks in South East Asia. Furthermore, BBC News, (2003) reported that South Korea, Australia, China, Taiwan and Japan have been the victims of hundreds of hack attacks causing millions of losses.

In Japan, the National Police Agency has revealed that the police computer networks have come under cyber attacks - a staggering 51,000 times from July till September 2002 (www.mdc.mainaichi,_2002). Gartnergroup highlighted that cyber criminals could dupe millions of online consumers in acts of "economic mass victimization" in the next two years (www.gartnergroup.com).

The economic impact and damage caused by the digital attacks have once again enhanced the awareness about the necessity of having a concrete and stringent cyberlaw in the country. To this end, some developing countries have established several cyberlaws in recent years (shown in Table 1 below).

Table 1: Cyberlaws in Selected Developing Countries

No	Country	Name of Cyberlaw
1	China	Regulation on Protecting the Safety of Computer Information 1994; Computer Information Network and Internet Security, Protection and Management Regulations 1997
2	India	Copyright Act 1957; Information Technology Act 2000
3	Philippines	Electronic Commerce Act, 2000
4	Thailand	Electronic Commerce Law
5	Malaysia	Copyright Act 1997; Computer Crimes Act 1997; Digital Signatures Act 1997; Telemedicine Act 1997; Communications and Multimedia Act 1998; Optical Discs Act 2000.
6	Indonesia	NA

Source: Urbas (2001)

2. AN OVERVIEW OF THE CYBERLAWS IN MALAYSIA

In this section, we provide an overview of the cyberlaws existing in Malaysia. Malaysia has long recognized the impending challenges brought in by ICT development. Among the most visible challenges in the information age is the integrity and security of information, privacy of information and intellectual property issues.

One of the first measures taken to counter cyber crimes in the country was the establishment of the Malaysian Computer Emergency Response Team (MyCERT) under

the authority of MIMOS, which addresses the issue of information security. It was reported that as at end of 2001, a total of 932 computer abuse cases were reported, involving mostly big corporations (Karim and Khalid, 2003).

As at end of 2002, Malaysia took one step further in addressing cyberspace challenges by enacting six cyberlaws, which are the Digital Signature Act 1997, Computer Crimes Act 1997, Telemedicine Act 1997, Communications and Multimedia Act 1998, Copyright (Amendment) Act 1997 and Optical Discs Act 2000.

Moreover, three new cyber bills are being drafted, namely, Private Data Protection Bill, the Electronic Government Activities Bill and the Electronic Transaction Bill. In the next ensuing sections, we will highlight imperative details of these laws in detail.

2.1 Digital Signature Act 1997

The Digital Signature Act was enacted in 1997 and was fully in operation on I October 1998. This Act was modeled based from the United Nations Commission on International Trade Law (UNCITRAL), an Act concerned with digital signatures.

The Digital Signature Act 1997 governs issues relating to the use of electronic communications and electronic commerce. It provides the legal effects of digital signatures and its underlying technology and of transactions entered into using digital signatures. Moreover, this Act also governs the functions, duties, rights and obligations of all parties involved in authentication and integrity services, which also includes the subscribers.

While one may think digital signatures as signatures made by utilizing digitized pens or pen-computers, which translates the actual handwritten signatures into an electronic format, but in actual fact any form of signature would constitute evidence linking a person to a document. Johnston et al., (1998) provides clear distinction between digital signatures and electronic signatures.

Lee (2002) describes a digital signature as a string of data generated by a cryptographic method that is attached to a message to ensure its authenticity as well as to protect the recipient against repudiation by the sender.

With the introduction of Digital Signature Act 1997, it is envisioned that there will a significant reduction in online transactions fraud cases in Malaysia. The Digital Signature Act is deemed to facilitate electronic commerce through legislation in the areas of digital signatures, cyber payments, and intellectual property protection. Among the most pertinent developments introduced by this Act are as follows:

- The legal definition of a digital signature.
- The legal recognition of electronic documents signed by a digital signature.
- The mandatory use of digital signatures for certain electronic documents.
- The establishment of licensed certification authorities.

- The statutory warranties and duties imposed on certification authorities and subscribers in relation to digital signatures.
- The distribution and apportionment of liability for digital signature fraud.

2.2 Computer Crimes Act 1997

In March 1997, Malaysia enacted the Computer Crime Act, which regulates computer related crimes such as unauthorized interception of programs or data over computers, computer systems and networks, hacking and virus spreading. This law is deemed important due to the increase in computer related transactions, especially financial transactions (e.g. electronic banking). This Act is similar to the United States Computer Fraud and Abuse Act 1986 (in the United States), the Computer Misuse Act 1990 (United Kingdom) and the Computer Misuse Act 1993 (Singapore). The ultimate objective of this Act is to deter computer crimes and provide protection to consumer's privacy. Generally, there are fours types of offences covered in the Act, which are as follows:

- Unauthorized Access: s.3
- Ulterior intent: s.4
- Modification of content: s.5 and
- Communication of codes or passwords: s.6.

Under this Act, the word 'computer' has been described 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 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" (Section 2 of the Act).

Meanwhile "*computer network" is* deemed to mean "the interconnection of communication lines and circuits with a computer or a complex consisting of two or more interconnected computers". In the event of the computer being housed outside the borders of Malaysia, the Malaysian government under this Act gains extra jurisdictional power (Shanmugam et al., 2002).

2.3 Telemedicine Act 1997

The Telemedicine Act was enacted in March 1997 to support successful implementation of the Telehealth flagship, which is one of the major objectives of the Ministry of Health. The central objective of this legislation is to regulate the practice of medicine through the use of multimedia.

This Act defines the categories of people who are qualified to practice telemedicine, as well as penalties for professional misconduct. However, this Act has little to do with the e-commerce activity. The Telemedicine Act 1997 must be read together with the Medical Act 1971 as telemedicine is the practice of medicine using a different technology. In a

nutshell, this Act provides the environment for the future development and delivery of healthcare in Malaysia.

2.4 Communications and Multimedia Act 1998

The local multimedia and content development landscape has changed drastically in recent years. Several years back, there was a clear distinction between the telecommunication, posts, broadcasting and printing industries and each of these industries was regulated by several different pieces of legislation, such as the Telecommunications Act 1950, Printing and Publications Act 1984 and the Broadcasting Act 1988. However, the old regulatory framework cannot cope with convergence and inhibits the growth of the new converged industry in the country.

Hence in 1998, the Communications and Multimedia Act was enacted to ensure the nation's policy objectives for establishing Malaysia as a communications and multimedia information and content services hub are met. The specific objectives of the Act are to:

- Promote the national policy objectives for the communication and multimedia sector.
- Establish a licensing and regulatory framework to support the national policy objectives for the sector.
- Establish the powers and functions for the Malaysian Communications and Multimedia Commission.
- Establish powers and procedures for the administration of the Act.

2.5 Copyright (Amendment) Act 1997

Technological development has also challenged governance of copyright issues in Malaysia. The first Copyright Act was established in 1987 to protect copyright works such as music, books and films. In subsequent years, this was repelled and amended, once in 1990, 1996 and the latest in 1997. However, while copying is punishable with heavy fines and/or imprisonment, copying for back-up purposes is not considered an infringement under Section 40 of the Act.

2.6 Future Cyberlaws

While we have recognized the existing cyberlaws in Malaysia, several other new cyberlaws are also in the pipeline. Currently, the government is drafting the Private Data Protection Bill, the Electronic Transactions Bill and the Electronic Government Activities Bill.

The Private Data Protection Bill will act as a complement to the Communications and Multimedia Act and the Digital Signature Act and regulate the collection, holding, processing or use of personal data by any person. Consumer confidence can be boosted as this Bill protects personal data hence ensures the privacy of individuals is not invaded. The Bill covers personal data relating directly to a living individual and applies to both automated and non-automated personal data files in the public and private sectors.

The purpose of the Electronic Transactions Bill is to facilitate the use of electronic means as a medium of communication to support the goal of the government of in promoting electronic commerce. The Bill tries to decrease compliance and transactions cost for both businesses and consumers and also remove existing legislative impediments to commercial transactions with the government through electronic means (Karim and Khalid, 2003). The Bill also reduces uncertainty and ambiguity pertaining to the legal effect of electronic messages and the time and place of dispatch and receipt of electronic messages.

This is consistent with countries that have adopted the principle provisions of the UNCITRAL Model Law on E-commerce. The Bill will also allow paper based legal requirements to be met by using electronic technology. The Electronic Government Bill was drafted to ensure the smooth implementation of electronic dealings between the government and the public. The dealings will be mainly through the Internet.

Most of the statutes regarding government dealings were drafted to suit a paper-based scenario therefore this Bill is necessary for the electronic based surroundings. The Bill will only be used for statues where there are express restrictions to electronic dealings.

3. CYBERLAWS – THE IMPENDING CHALLENGES

Malaysia has taken great efforts in the enactment of cyberlaws to regulate cyber crimes in the country. However, the implementation of such laws also faces several challenges, which requires diligent and serious concern. Some of the major issues confronting current laws are discussed below.

3.1 Lack of Territorial Borders in Cyberspace

According to Branscomb (1996), cyberspace is not one distinct place but many cyberspaces with numbers of models from the real world that are replicated in computer-mediated communication. Cyberspace transcendences geographical borders - due to the minimal cost of information transfer. The challenges for the law are created by the cross boundary nature of cyberspace. Physical borders are not simply arbitrarily created, although they may be based on historical accident, geographic borders make sense in the real world. This also relates to the issue of jurisdiction or the authority of a court to hear a case and resolve a dispute within a sovereign territory (Edappagath, 2001). This is because cyber cimes is not limited within certain geographical location. Thus, the source or origin of the fraud being commited is often difficult to ascertain.

3.2 Consumer Protection

The introduction of a new financial delivery system provides consumers with alternatives and opportunities although gives rise to certain concerns such as breadth of service access, health of service providers and consumer privacy (Brewer and Evanoff, 2000). Protection is of utmost importance for consumers when engaging in financial

transactions. Privacy and confidentiality of information are the most common consumer protection.

The digital aspects of technology have brought new challenges to the law. Today, hackers are now well equipped in neutralizing any encryptions used to protect sensitive data. Hackers are so advanced that they appear to outsmart their security counterparts most of the time. Lawmakers' attempts at forming new legislation have been hampered by technocratic lawyers who carefully exploit loopholes to circumvent these new laws. In other words, the constant evolution of technology would bring in new form of challenges to lawmakers.

3.3 Intellectual Property Issues

Intellectual property comprises four main types of intangible property, which are patents, trademarks, copyrights and trade secrets. Intellectual property is an asset that can be bought, sold, licensed or exchanged therefore sharing the same characteristics as real or personal property. However, intellectual property is non-physical and in the normal world (non-cyberspace), this poses significant problems. The problem is worse as in cyberspace as intangibility is just electronic impulses and nothing else. International agreements on establishing effective copyright, patent and trademark protection are vital in order to combat piracy and fraud. An adequate and effective legal framework is also necessary to support efforts in preventing fraud and theft of intellectual property.

4. CONCLUSION

Malaysia has been making much progress in creating a safe and sound cyber environment with the establishment of several set of cyberlaws. However, this is only the beginning of a long journey. The rapid development of ICT in the new economy requires constant reviewing and enactment of new cyberlaws. Moreover, cybercrimes are borderless – it can happen at any time and from anywhere in the world. Thus, it is important for each jurisdiction of the cyberlaw to be continuously updated and reformed.

In addition, the public need to given ample awareness on the cyber crimes and the cyberlaws, as it is important for the public to know their rights and limitations in the information age. This also creates confidence and trust on the electronic based activities such as electronic banking, insurance and stock trade. Further, strategic international cooperation is also needed to combat cross border cybercrimes. As for now, the knowledge that a legal framework for cyber activities has been established so that online activities can proceed further is encouraging enough.

REFERENCES

Branscomb A. W. (1996), "Cyberspaces: Familiar Territory or Lawless Frontiers", Journal of Computer-Mediated Communication, Volume 2, Number 1, available at www.ascusc.org/jcmc/vol2/issuel.

Brewer III E. and Evanoff, D. D. (2000), "Changing financial industry structure and regulation", Chicago Federal Letter, Chicago, September, p. 1-5.

Brynjolfsson, E. and Hitt, L. (1995), "Information Technology as a Factor of Production: The Role of Differences Among Firms, *Economics of Innovation and New Technology*, Vol. 3, No. 4, (Special Issue on Information Technology and Productivity Paradox) pp. 183-200.

Colecchia, and Schreyer, P. (2002), "ICT investments and Economic Growth in the 1990s: Is the US a Unique Case?: A Comparative Study of 9 OECD Countries", *Review of Economics Dynamics*, Vol. 5, pp.408-442.

Council of Europe (2001), *Draft Convention on Cybercrime* (Final Draft and Explanatory Note), European Committee on Crime Problems and Committee of Experts on Crime in Cyberspace, Strasbourg, 29 June 2001, see http://www. conventions.coe.int/treaty/EN/projects/projects.htm

Duggal, P. (2001), *Cyberlaws: Evolving Practices*, ADB Regional Roundtable, 29th August 2001.

Edappagath, M.A (2001), "Cyberlaws in Information Age", paper presented at *Asia Pacific Regional Workshop on Equal Access of Women in ICT*, Seoul, R.O. Korea, October 22-26, 2001.

GartnerGroup (200 1), 'Rethinking on Cyber crimes' www.garnergroup.com

Gourova, E., Ducatel, K., Garigan, J. and Scapolo, F., (2001), "Knowledge, Technology and Learning Capabilities", *IPTS Working Paper.*

Grabosky, P.N. and Smith, R.G. and Dempsey, G. (2001), *Electronic Theft: Unlawful Acquisitions in Cyberspace*, Cambridge University Press, Cambridge.

Johnston, D., Handa, S., and Morgan, C., (1998), Cyber Law, Pelanduk Publications.

Karim, M.R. and Khalid, N.M., (2003), E-Government in Malaysia, Pelanduk Publication.

Lee, M. P., (2002), Law on Banking and Finance - Study Manual, IBBM Publications.

OECD (2001), *The New Economy: Beyond the Hype*, The OECD Growth Project.
Shammugam B., Ramasamy, S. and Balachandher K.G., (2002), Malaysian Regulation vs. E-Banking, *Journal of International Banking Regulation, Vol.* 4, No. 1, August 2002.

Urbas, G. (2001), *Cybercrime Legislation in the Asia-Pacific Region*, Australia Institute of Criminology, Canberra.

www.mdn.mainichi.co.ip/news/2000

www.news.bbc.co.uk