VIOLATION OF CYBERLAWS AND COMPUTER ETHICS: THE CONSEQUENCES AND POTENTIAL LEGAL ACTIONS

Juriah Abdul Jalil & Duryana Mohamed
Department Of Private Law,
Ahmad Ibrahim Kuliyyah Of Laws
International Islamic University Malaysia. Malaysia
juriah@iium.edu.my & mduryana@iium.edu.my

Abstract

Good ethics and professionalism when using computer or Internet should be strictly observed and exercised. Failure to do so will result in violation of the laws and computer ethics. Consequently, not only the victim will suffer loss but also the country as a whole. It is known that, the borderless nature of the cyber world has encouraged many people to try and explore various types of cyber activities but that is not a passport for everybody to cross the border and ignored the laws and regulations. Although there are cyber laws to control and regulate these cyber activities cases of cyber attacks and invasion to privacy and safety are still rampant. Thus, this paper seeks to study the available laws governing computer users, cases that involve violation of cyber laws and computer ethics, the effect of violation of those laws on the victim and finally, the potential legal actions available tothe victim of cyber attacks according to the categories of the offences. References will be taken from various discussion on cyber and computer ethics as well as cases on cyber offences. In conclusion, the authors hope that this paper would be able to assist the victims to stand up for their rights by seeking the available remedies besides providing resources to lawyers and court officers in dealing with cases on cyber attacks, particularly in Malaysia.

1.0 Introduction

Cyber world is known for its unlimited space and boundaries. Thus, anyone can upload anything into the unlimited space from anywhere in the world. Consequently, cyber world become an ocean of information that enables people to share, communicate, make business, making friends including creating opportunities to commit crimes and taking advantage of people openness in sharing data and information about themselves by those predators looking for victims in the cyber world. Regulating behaviour is never easy despite the existence of laws and regulations and one of the most difficult challenges is that technology are often too fast developed for the law to catch up. Nevertheless, observing computer ethics and respecting privacy of other people should be imposed and be made aware to all online users. However, most importantly to the victims is the availability of a legal redress to compensate the loss suffered as a result of abuse and violation of the laws by the criminals.

This paper will highlight the available laws that govern the computer users and cyber activities. Several selected cases on violation of the cyber laws and computer ethics will then be analysed. The effect of violation of those laws on the victim and their rights to sue for damages and other remedies will be presented at the later part of this paper. The aims are to provide information to the victim of cyber attacks and to provide further references to lawyers and court officers in dealing with cases on cyber attacks, particularly in Malaysia.

2.0 CYBERLAWS AND COMPUTER ETHICS

Law in general terms means to regulate and govern in order to create a safe environment. Thus cyberlaws are set of laws that govern or regulate the cyber activities. In relation to formation and enactment of cyber laws in Malaysia, Tun Mahathir Mohamed who was the former Prime Minister of Malaysia, explained that the reason for enacting various cyber laws were intended to prevent destructive abuses. This is an important step in order to promote and create a positive and progressive development of cyber activities in Malaysia that will benefit both the country and citizen at all age.

The term, 'ethics' refers to the rules and standards governing the rightful or wrongful behaviour of an individual and it defines what is good for the individual and for society and establishes the nature of duties that people owe themselves and one another.

In relation to cyber world, a new type of ethics known as computer ethics has emerged resulting in the creation of Code of Computer Ethics that may have binding effect on the professionals particularly if the code becomes part of the work ethic and procedure. Failure to comply with the Code may lead to violation of the laws or breach of employment contract.

In order to govern the computer ethics, the Computer Ethics Institute of the United State has created the Ten Commandments of Computer Ethics in 1992 that read as follows:

1. You shall not use a computer to harm other people
2. You shall not interfere with other people's computer work
3. You shall not snoop around in other people's computer files
4. You shall not use a computer to steal
5. You shall not use a computer to bear false witness
6. You shall not copy or use proprietary software for which you have not paid
7. You shall not use other people's computer resources without authorization or proper compensation.
8. You shall not appropriate other people's intellectual output.
9. You shall think about the social consequences of the program you are writing or the system you are designing.
10. You shall always use a computer in ways that ensure consideration and respect for your fellow human.

Other than the Association for Computing Machinery (ACM), the British Computer Society has also published a code of conduct and code of practice for computer professionals in the UK. In Malaysia, a code known as Content Code has been created. The content Code sets out the guidelines and procedures for good practice and standards of content disseminated to audiences by service providers in the communications and multimedia industry in Malaysia. The Code seeks to identify what is regarded as offensive and objectionable while spells out the obligations of content providers within the context of social values in this country. This code put the responsibility of the contents of the internet on the creator of content.

2.1 Violation Of the laws and Computer Ethics

Violation of laws may include violation of computer ethics but violation of computer ethics may not be necessarily amount to violation of the laws in some countries. This is due to different concepts of ethics adopted by the countries. Nevertheless ethical values and legal principles are usually closely related. In some cases the law mandates ethical values particularly in employment sphere and in supporting self regulation in case of media and telecommunication industry, by setting up the code of ethics. Based on the Ten Commandments of Computer Ethic, the law actually codify these ethics in the manner of protecting the reputation, privacy, information and data, copyright and other fundamental rights and liberties of other human being in the cyber world. Most of these laws are now being extended to apply to online matters. In the absence of relevant law to govern certain online matters, cyber laws have been enacted which also provides punishment for violation or breach of any rights of a person.In Malaysia, there are several laws governing cyber activities and the laws were enacted by the government since 1997.

2.2 The Cyberlaws and its Scope

The cyberlaws were enacted with the objectives of governing the cyber activities and to control any cyber attacks. The laws also provide specific punishment for the cybercriminals. However, not all laws provide adequate protection to the computer users. The followings are the laws and their objective:

a) *Computer Crimes Act 1997:* The aim of this Act is to govern offences relating to misuse of computers, including through networking and electronic mail. There are 12 sections in the Act. This Act provides criminal sanctions or punishment.

b) *Copyright (Amendment) Act 1997:* This Act aims to protect against the unauthorised transmission of copyright work on the Internet and to deal with issues on software piracy, infringement of online trademarks, domain names dispute and new invention of patents. Other relevant Acts include Trade Marks Act 1976, the Patent Act 1983, the Industrial Design Act 1996, the Layout Designs of Integrated Circuits Act 2000 and the Optical Discs Act 2000. Most of these Acts mentioned here provides for civil remedies for infringement of the owner's right. The Optical disc Act nevertheless provides for criminal punishment.

c) *Communication and Multimedia Act 1998:* This Act has been enacted to govern and guide the development of this multimedia industry. The Act is based on the principles of transparency and clarity, flexibility, competition and industry self-regulation. There are also many rules, regulations and exemption orders governing the industry in Malaysia, which have been created due to innovations and inventions in the communication and broadcasting industries. There are several sections governing cyber related cases namely sections 112 and 233.

d) *Digital Signature Act 1997:* The Act aims to provide security protection to online transactions. It regulates the use of digital signatures and governs certification authorities through issuance of valid licences. It only legalises one form of digital signature technology, namely private key-public key Cryptography (PKP).

e) *Telemedicine Act 1997:* This Act provides for regulation and control of the practice of telemedicine in Malaysia with the aim to improve the healthcare services of society through ICT. The Act also emphasises on the importance to obtain patient's consent before giving him any medical treatment.

f) *Communication and Multimedia Commission Act 1998 (CMCA)*: This Act has been enacted to oversee the development of the communication and multimedia industry through the creation of a Multimedia Commission. It also lists down several aims and national policy objectives in section 3 of the Act.

g) *Optical Discs Act 2000 (ODA):* This Act provides for the licensing and regulation of the manufacture of optical discs to combat piracy. It is used to prosecute criminals who produce illegal copies of protected movies and music.

h) *Electronic Commerce Act 2006:* The aim of the Act is to boost electronic commerce activities in and to enable Malaysian business activities to compete in the global economy. It also provides legal recognition for electronic communications, electronic signatures and electronic documents.

i) Electronic Government Activities Act 2007 (Act 680): This Act applies to Federal laws and legalizing the use of electronic message when dealing with the government. However, such use is not compulsory to any person unless he consented to that method. There are also certain legal requirements to be fulfilled by such electronic message. An Order was also passed in May 2010 and known as Electronic Government Activities (Prescription of Electronic Signature) Order 2010.

j) Personal Data Protection Act 2010: This Act applies to any person who processes and any person who has control over or authorizes the processing of any personal data in respect of commercial transactions. It also provides protection on the rights of data subject/data users.

2.3 Cyber activities, offences and consequences of violation of those laws

Cyber offences refer to offences committed using electronic means or by way of internet. The medium includes hand phone and other electronic gadgets. Offences such as online defamation, online child pornography, hacking, computer fraud, phishing or identity theft and violation of privacy are among cyber attacks that had given bad effect to the society, economy and politics of certain countries.
Blogging is one of the most active cyber activities that may expose bloggers to online criminal defamation suits and civil defamation suit. Bloggers may also be suit for infringement of copyrights.

2.3.1 Blogging, Online Criminal Defamation and sedition

Blogging is common nowadays but the bloggers must know the limits and restriction when communicating in the internet. The following laws may be used to charged and prosecute bloggers namely:

i. Internal Security Act 1960
ii. Sedition Act 1948
iii. Sec 499 of Penal Code – criminal defamation
iv. Sec 112 and Sec 233 of Communication and Multimedia Act 1998

Section 112 may be applicable to bloggers who tend to publish any obscene material such as pornography or offensive materials. But, the section has not yet been tested in the court of law.

According to sub-s (1) of section 112, 'no content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person'. Sub-section (2) of the same section furthermore states that 'a person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day or part of a day during which the offence is continued after conviction'.

Another relevant section is s 233 which provides that;

(1) A person who -- (a) by means of any network facilities or network service or applications service knowingly -- (ii) initiates the transmission of, (a) any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or (b) initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address, commits an offence.

(2) A person who knowingly - (a) by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or (b) permits a network service or applications service under the person's control to be used for an activity described in paragraph (a), commits an offence.

(3) A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day during which the offence is continued after conviction.

Bloggers that has been charged under these provisions includes Raja Petra Kamaruddin who is also an editor of *Malaysia Today*, a blog popular for its political postings and critiques of alleged Wrong doing by public officials. He was arrested on September 12 under section 73(1) of the colonial era Internal Security Act 1960 (ISA) for allegedly being a threat to security, peace and public order.

He was arrested a day after a two-week block on his website was lifted. Petra was given a two-year detention order under section 8(1) of the ISA on September 23.

In Singapore a blogger, Gopalan Nair who is an American citizen and a former Singaporean lawyer was sentenced to three months imprisonment on September 18, for 'insult' under article 228 of Singapore's Criminal Code. He was initially arrested on May 31 under article 13D of the Miscellaneous Offences Act. Four days after his arrest, he was charged with 'sedition' for criticizing two judges on his blog. In fact, a week before Nair's sentence was handed down, the attorney general initiated contempt of court proceedings against the publisher of the Asian edition of the *Wall Street Journal* and two of its editors on the allegation that their editorial "impugn the impartiality, integrity and independence of the Singapore judiciary". Both were sentenced to jail terms of 12 and 10 days respectively for contempt of court on 3 June 2008.

Other cases involving bloggers include six bloggers who were charged for insulting the Sultan of Perak' and a former EON Bank Bhd employee, Seah Boon Khim, who pleaded guilty in the Sessions Court for posting an obscene blog title to embarrass his former boss. He was fined RM8,000 and in default two months jail by the Sessions Court.

2.3.2 Online child pornography

This offence is committed by using and targeting children as victim since they are easy to be influenced by cyber criminal. In the US Child pornography has long been treated severely under both federal and state law. The following Acts has been enacted to prevent online child pornography:

1. Child Pornography Prevention Act (CPPA) of 1996, designed both to close loopholes in existing federal child pornography law and address new technological issues by the following:

- Criminalizing the act • of knowingly possessing, selling, receiving, sending, or transmitting child pornography via the internet or e-mail.
- Criminalizing so-called "virtual" depictions of child pornography, those that appear to involve minors and those created by computer graphics software.

2. The Protection of Children from Sexual Predators Act of 1998 contains further anti-child porn provisions. Title II of the law contains the following provisions:

- Provides for the prosecution of individuals for the production of child pornography if the visual depiction was produced with materials that have been mailed, shipped, or transported in interstate or foreign commerce, including by computer.
- Tightens previous federal law by making it a criminal offense to possess for even one depiction of child pornography
- Outlines responsibilities for Internet Service Providers in reporting child pornography to Authorities
- Increases federal criminal penalties for child pornography, which include fines and prison sentences ranging from 15 to 30 years

3. The Protection Act of 2003

- Known as AMBER Bill America's Missing: Broadcast Emergency Response that prohibits virtual children pornography. It allows federal law enforcements to use

nationwide emergency system to alert the public about missing children, and wiretappping and electronic surveillance in the investigation of children pornography.

4. Child Online Protection Bill (COPA)

- The Bill has the purpose of restricting access by minors to any material defined as harmful to such minors on the Internet. The United States Federal Courts have ruled that the law violates the constitutional protection of free speech, Therefore have blocked it from taking effect. COPA required all commercial distributors of "material harmful to minors" to restrict their sites from access by minors. "Material harmful to minors" was defined as material that by "contemporary community standards" was judged to appeal to the "prurient interest" and that showed sexual acts or nudity (including female breasts). This is a much broader standard than obscenity.

2.3.3 Hacking

This offence involves unauthorised access to other's computer system. The hacker may be charged either under section 3 or sec 4 of the Computer Crime Act 1997. Section 3 deals with unauthorized access offence while section 4 deals with unauthorised access with intent or aggravated hacking. The penalty for offence committed under section 3 is liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both while section 4 emphasis on the unauthorised access with the intention to commit fraud or dishonesty or to cause injury as defined by the Penal Code. Nevertheless the Act is silent on the punishment for repeated offences. Stiffer punishment is provided under sec 4 in the amount of fine not exceeding one hundred and fifty thousand ringgit or face imprisonment for a term not exceeding ten years or both.

2.3.4 Computer fraud

This financial crime is a traditional crime but now it may be committed via internet. There is no specific cyberlaw provision in Malaysia governing this crime but the suspect is usually investigated according to Criminal Procedure Code and charged under the Penal Code. Other than the laws, there is a need for financial institutions to adopt integrated approach in fighting the crime where in the industry, the technology experts and the enforcement agency should work together.

2.3.5 Identity theft or Phishing

An identity theft is also known as phishing. This crime usually involves online or Internet banking whereby the fraudsters will send dubious e-mails or create spoof websites hoping to entice users to hand over their credit card or banking details. There is no specific provision of law on this type of crime but this crime could cause billions of losses.

2.3.6 Privacy

Privacy can be defined as a right to be alone and free from any disturbance. There are many types of privacy such as information privacy that requires data protection law to protect it, bodily privacy, privacy of communications and territorial privacy. The law that may be applicable is the Personal Data Protection Act 2010. For violating one's privacy, a person can be charged under Section 509 of the Penal Code which provides criminal penalties for insulting the modesty of any person or intruding upon the privacy of [any] person by uttering any word, sound or gesture, or exhibiting any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen by such person.

2.4 Effects of cyber offences and the remedies available for victims

Cyber laws enacted in Malaysia provide for criminal punishment against cyber offenders. Cyber laws as seen above provide stiffer punishment in the form of imprisonment and fines. This nevertheless will benefit not be sufficient redress for the individual victims. Thus what kind of remedies available for the victims? Most judicial system has two system of justice namely the criminal justice system and the civil justice system. While criminal justice determines the guilt or innocence of the offender, civiljustice system ascertains whether the wrong doer is liable for the injuries suffered by the victims.

a. For online defamation – the victims suffers injury to reputation and thus may claim for damages as provided under the Defamation Act 1957 and an injunction may be sought to prevent further or repeat publication of the defamatory message.

This signifies that a blogger or any person who published defamatory words online may be subjected to two types of legal suit namely criminal defamation and the other is civil defamation.

b. Hacking – unauthorised access to the computer system may entitle the victims to have remedies provided under the law of torts such as:
i. trespass into property
ii. intrusion
iii. breach of duty if it is committed by employee who has no authority to obtain the information

c. Computer fraud – in cases involving a fraudulent investment scheme for example, the victims may apply for mareva injunction to freeze the assets and prevents the scammer from having access to the assets pending disposal of the case in court. The Court in Canada for example has authority to issue a 'worldwide' mareva injunction to preserve assets which are physically located outside the court's jurisdiction. Mareva order may also be issued against any financial institution which was believed to have the scammer's accounts within the institutions. The application must be made promptly in order to stop the scammers from dissipating with the assets.

d. Identity theft or phishing. The victim may sue for loss suffered by him nevertheless the cause of action must be clearly established.

e. Privacy – Privacy is not recognised in Malaysia nevertheless it argued that privacy right should be recognised as one of the important principles under human rights. Islam however recognisedand protects individual privacy. With the enactment of Personal Data Protection Act 2010, this may be the basis for civil action that involved infringement of personal data.

3.0 CONCLUSION

There are several laws governing the cyber world that computer users should be aware of. While ethics guide the behaviour of computer users, the law regulate and impose punishment for offender and those who abuse, manipulate and misuse the usage of computer and the internet. Nevertheless the most effected is usually the victims, the possible solution would be taking civil actions against the wrong doer and claim for damages for the loss suffered

.

REFERENCES

Abu Bakar Munir & Siti Hajar Mohd. Yasin, 'Would the phishers get hooked?'. Paper presented at 22nd BILETA Conference, 16-17 April 2007, Hertfordshire.

Aishath Muneeza, The milestone of blogs and bloggers in Malaysia, [2010] 3 MLJ cvii.

Association for Computing Machinery, Inc. Association for Computing Machinery: Code of Ethics. http:// en.wikipedia.org/wiki/Computer_ethics, accessed on 16th July 2010.

"Cybercrimes cost billions in losses", *New Straits Times (Computimes) Online*,1 MMarch, 2004. http://www.ctimes.com.my/

Computer ethics and legal issues at http://www.freewebs.com. Association for Computing Machinery, Inc. Association for Computing Machinery: Code of Ethics

Dr Mahathir bin Mohamad, Foreword note in Abu Bakar Munir. Cyber Law, Policies and Challenges, 1999. Butterworth Asia. Kuala Lumpur.

G Jack Bologna and Paul Shaw, *Avoiding cyberfraud in small businesses: what auditors and owners need to know*, at 61.

Halim Shafie, "*Updates on the Malaysian cyber laws framework,"* 3rd International Cyber laws Conference: Advancing Cyber laws: educate, regulate, practice and enforce, 2-3 March 2004, Kuala Lumpur. For further information see the MCMC, http://www.mcmc.gov.my/the_law/legislation.asp accessed on 13 June 2005.

Halim Shafie, "*Updates on the Malaysian cyber laws framework,"* 3rd International Cyber laws Conference: Advancing Cyber laws: educate, regulate, practice and enforce, 2-3 March 2004, Kuala Lumpur. For further information see the MCMC,

http://www.mcmc.gov.my/the_law/legislation.asp> viewed on 13 June 2005.

http://en.wikipedia.org/wiki/Computer_ethics retrieved 16th July 2010.

http://www.acm.org/about/code-ofethics

http://en.wikipedia.org/wiki/Computer_ethics retrieved 16th July 2010.

http://en.wikipedia.org/wiki/Cyberlaw

http://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics retrieved 16th July 2010. See also http://www.freewebs.com

Jo Timbuong, Integrated Solution needed to fight fraud effectively, InTech, the STAR, 3rd August 2010 at IT18.

Joanna Loy, Privacy: Des it exist in Malaysia? Is it time to legislate?, 11 March 2009 at http://www.malaysianbar.org.my retrieved 22 July 2010

Joseph Loh, Tweet below the Law, Sunday Star, 8 August 2010 F17.

Julian Ding, *E Commerce: Law and Practice*, Sweet & Maxwell Asia, 1999, at 201 and Zinatul Ashikin A. Zainol,
"Electronic commerce: A comparative analysis of the Malaysian Digital Signature Act 1997 and the Singapore Electronic Transaction Act 1998," 15th BILETA Conference; "Electronic Datasets and access to legal information",
14th April 2000, http://www.bileta.ac.uk/00papers/zainol.html viewed on 14 November 2002.
Mageswari, M, 2009, *IT Auditor Pleads Guilty to Slamming his Ex-boss in Website*at http://thestar.com.my/news/ story.
Margaret A Healy, "Child pornography: An international perspective", 2 August 2004, via Computer Crime Research Center (CCRC), http://www.crime-research.org/articles/536
Meryam Dhaboiwala, Legal system used to silence bloggers, suppress freedom of expression at http://www.ethicsinaction.asia/archive/2008-ethics-in-action/vol.-2-no.-5-october-2008/legal-systems-used-tosilence-bloggers-suppress retrieved 23 July 2010.
N Ben Fairweather, ' Commentary on the ten commandments for computer ethics' at http://www.ccsr.cse.dmu.ac.uk/resources/professionalism/codes/cei_command_com.html retrieved 16th July 2010
Navaseelan Balasingam v *Public Prosecutor* [2007] 1 SLR 767.- on illegal withdrawal from ATM machines.
Nehaluddin Ahmad, 'Truth about identity fraud: Defence and safeguards', [2009] 9 CLJ i.
Nehaluddin Ahmad, The right to privacy and challenges: A critical review, [2008]5 MLJ cxxi
Ramon C. Barquin "In Pursuit of a 'Ten Commandments' for Computer Ethics" http://en.wikipedia.org/wiki/
Ten_Commandments_of_Computer_Ethics, accessed on 16th July 2010
Sabrina Mohamed Hashim, Blogging - Are You Exposing Yourself To Legal Liabilities? [2007]2 CLJ i
Shah, AS, *Six Charged for Insulting Perak Sultan*at http://sultanazlan shah.blogspot.com/2009/02/six-chargedfor-insulting-perak-sultan.html.
Supt Lim Hong Shuan, White –Collar Crime in Malaysia at http://mpk.rmp.gov.my/jurnal/2005/ whitecollarcrime.pdf retrieved 23 July 2010.