COMPUTER CRIME: A COMPARATIVE STUDY BETWEEN ISLAMIC AND MALAYSIAN LAW

DZULKEFLY BIN MOHED

UNIVERSITI SAINS ISLAM MALAYSIA

COMPUTER CRIME: A COMPARATIVE STUDY BETWEEN ISLAMIC AND MALAYSIAN LAW

Dzulkefly Bin Mohed
(Matric No. 1040698)

Academic project report submitted in partial fulfillment for the degree of
BACHELOR OF SYARIAH AND JUDICIARY
WITH HONOURS

Faculty of Syariah and Law
UNIVERSITI SAINS ISLAM MALAYSIA
Nilai

May 2007

AUTHOR DECLARATION

بسم الله الرحمن الرحيم

I hereby declare that the work in this academic project is my own except for quotations and summaries which have been duly acknowledged.

Date: 9th May 2007

Signature : .....
Name : Dzulkefly bin Mohed
Matric No : 1040698
Address : Lot 246, Kampung Sri Langkas, Batu 13, 47100, Puchong, Selangor Darul Ehsan.

ACKNOWLEDGEMENT

بسم الله الرحمن الرحيم

Praise is to Allah, Peace and Blessing is upon our Prophet Muhammad and His Family, All His Companions and Followers.

Gratitude to Allah for giving His servant the opportunity to undertake and complete the academic project.

I would like to take this opportunity to express my profound gratitude and appreciation to Encik Arif Fahmi bin Md. Yusof, for his patience, supervision, and advice, in bringing this academic project into completion. My sincere thanks also go to all the lecturers, tutors, and staff of the faculty for their kind assistance in gathering the information for this research.

Futher, all thanks extended to the librarians of Islamic Science University of Malaysia (USIM) Library, National University of Malaysia (UKM), the International Islamic University of Malaysia (IIUM), the Islamic Centre Library (Kuala Lumpur) for their help at every stage in the collection of materials.

This academic project is also dedicated to my beloved parents, Mohed bin Jaafar and Aisyah binti Dehiri, and the rest of my family for their unconditional support and encouragement. All of you will always in my heart.

Finally, I express my gratitude to all my friends and everybody who have directly or indirectly assisted me during the completion of this research. Without your assistance, this research may be not finished. May Allah Bless you...

Gracious....

ABSTRAK

Kajian ini merupakan kajian mengenai jenayah berkaitan komputer yang berlaku di Malaysia menurut pandangan undang-undang Malaysia dan pandangan dari kaca mata Islam. Sejak kebelakangan ini. kadar jenayah yang berkaitan dengan penggunaan komputer telah meningkat secara mendadak di Malaysia. Kajian ini bertujuan untuk mewujudkan kesedaran masyarakat kerana wujudnya banyak kes jenayah komputer di Malaysia. Untuk memperolehi data, beberapa teknik kajian telah digunakan seperti kajian perpustakaan iaitu dengan merujuk kepada bahan cetak dan data-data yang berkaitan. Hasil kajian ini mendedahkan bahawa wujudnya undang-undang berkenaan jenayah komputer, namun tidak banyak kes yang dilaporkan di Mahkamah atas sebab yang tertentu. Dapatan dari hasil kajian ini juga membuktikan bahawa jenayah komputer tidak diterima dalam agama Islam berdasarkan kepada dalil-dalil yang dikaitkan dengan masalah jenayah komputer ini.

ABSTRACT

This project paper is a research on comparative study of computer crime between the Malaysian Law and Islamic perspective. Recently, the number of crime related with computer is increasing rapidly in Malaysia. This research aims to give a realization to the society effects from the increasing number of crime regarding computer in Malaysia. Library based research by referring to the relevant documents and data were the tools employed for gathering purpose. The findings indicate that there is law regarding the computer crime but there are a little number case has brought in to the court. And finally, the study concludes that the computer crimes also are not permissible in Islam and contradict with goals of syariah.

ملخص البحث

يناقش هذا البحث حول الدراسة المقارنةِ عن الجريمة الحاسوب بين القانون الماليزيِ والمنظور الإسلاميِ. الآن، نجد كثير الجريمة التي تتعلق بالحاسوب قد انتشرت بسرعة وبدون الحد في ماليزيا. ويهدف هذا البحث لإعْطاء الإدراك عن اثاره المفسدة الى المجتمع. وفي هذا البحث، استخدم الباحث المنجهي الرئيسي وهو الطريق الاستقرائي. الخلاصة، هناك يوجد القانون المتعلقة بالجرائم الحاسوب ولكن قليل في التهمة في المحكمة. وأخيراً، كان الجريمة الحاسوب لايسمح في الإسلام وهو يخالف بمقاصد الشريعة والدليل التفصيلية التي يبنى عليه الحكم في الإسلام.

CONTENT PAGE

LIST OF STATUTES

LIST OF APPENDICES

GLOSSARY

Dalil	Point out, indicate.
Fuqaha	Islamic Jurist.
Hadith	Saying of the Prophet.
Hukm	Legal rule.
Ibid	Latin words means "in the same place".
Ijma'	Consensus of opinion of the ulama'.
IP	Internet Protocol.
s.a.w	Abbreviation of "*Sallahu 'alaihi Wa Sallam*" meaning "peace be upon him". It is strongly encouraged for a Muslim to utter this blessing whenever he hears the Prophet Muhammad's name is being mentioned.
Surah	Chapter of the al-Quran. The number proceeding colon denotes the chapter number while the numbers after the colon denotes the verse number.
Syariah	The way of Islam.
Ulama'	Islamic Jurists.

ABBREVIATION

etc.	et cetera/and so on
i.e	id est/that is to say
ibid	ibidem/as previously mentioned
n.a	no author
n.d	no date
n.pl.	no place
n.pb.	no publisher
p.	page
pp.	pages
s.a.w	salla Allah ‘alayh wa sallam
s.w.t	subhanahu wa ta‘ala
vol	volume

CHAPTER ONE

CHAPTER ONE

INTRODUCTION

1.1 Background of Research

The advent of computer technology has brought many kinds of opportunities and some these, not surprisingly are of a criminal nature. Computers may facilitate the commission of "old-fashioned" crimes such as fraud or give rise to new mischief such as computer hacking and the deliberate erasure of programs or data. Contrary to popular belief, the law is reasonably well equipped to deal with computer crime and has been substantially strengthened by the Computer Crime Act 1997. The biggest stumbling block, in practical terms, is detection and considerable amount of thought must be given to the security of any computer system as, in this case, prevention better than cure.

Looking for the topic, the specific research also will look at the view of Islam about the computer crime. It is true that no direct power said about the computer crime. In this research, it may use the *qias* and what ever method that can be use as an authority on the computer crime.

Even though there are so many articles, books and discussion had made which discussing this issue, the writer feels that this research must take its part as the additional articles towards exposing the computer crime in Malaysia and the view of Islam about it.

Nowadays, referring to the situation involving with the computer crime in Malaysia, there are so many type of crime that happens in Malaysia. The writer feels that the exposure of the computer crime especially in Malaysia is needed because as a development country, Malaysia must face all of the challenging that must be face by the other develop country including Malaysia.

The type of computer crime is broad. As an example of the computer crime is the robbery by using the Auto Teller Machine (ATM) in the bank, using the pirate product such as not original software for the accessories of the computer including antivirus, program, hardware, software and other.

1.2 Aim of Research

Basically, the research will focus to the issue of computer crime according to the Malaysian Law and the view of Islam about it. There is relation between the computer crime and the cyber crime but it is different. The research will not discuss about the cyber crime deeply but only in general.

1.3 Objective of Research

There are some objective referring to this research and it is:

1. To overcome the historical background of computer crime according Malaysia Law.
2. To recognize acts and enactments involved about the computer crime.
3. To identify the acts and enactment that involve about the computer crime.
4. To emphasize the role that has and had played by laws about all matter of the computer crime.
5. To search the view of Islam about the computer crime.
6. To know the various issues had occurred and what will happen because of the problem.
7. To suggest an idea as solution against issue which arise.

1.4 Significance of Study

The writer thinks that the research is very important because there are a few exposures about the computer crime law in Malaysia. Beside of that, the writer also feels that not many people know about the computer crime law according Malaysian law. Then, the writer wants to know about the difference view from the Malaysian law and Islamic view about the computer crime. It is very useful as a room for improvements to know both of it. It is hoped that form this research the society will have clear view about the computer crime according to Malaysian law and Islamic view.

1.5 Scope of Research

The discussion of the research is about the computer crimes that happen in Malaysia through the laws and the Islamic Perspective. This research will focus deeply on the view of the computer crime in Malaysian Law and the differences between it and Islamic view. It also will discuss about the Act 1997 that is the main sources for the problem of computer crime in Malaysia. The matters in the Act are including the background of the creation and the brief content of provision in the Act.

Therefore, this research touch all cases, acts, enactments, journals and more relevant article which had discussing either specifically or generally either under the topic of computer crime in Malaysia. It will be more discussion on the computer crime in Malaysia and the view of Islam of it. We know that the computer crime have no any offence in Islam. It is because it is the latest problem. But, even there is no straight offence in Islam, the Islam have the special way about it. It is by *Qias* and other method.

Meanwhile, there will come out with relevant suggestion as the best solution combining the idea throw by scholars and academician that the effect after introducing the Act 1997. This research is not doing as the platform to present just about the computer crime in

Malaysian law and Islamic perspective. But, it do in sense to show the real scenario about it including the problem in Malaysia where need some repairing on it.

1.6 Research Methodology

Research design will be do by library-based method which relay on information in law books, law journals, cases reported, acts, enactments, law historical books, law nets, and law articles. These sources of library- based will found either in library or Internet. Because of this research discussed about Islamic matter in some part, some sources are in Arabic language will be use by translation which able to understand.

These are the library was visited by the author to complete the research:

i. Perpustakaan Negara Malaysia, Kuala Lumpur.
ii. Perpustakaan Universiti Sains Islam Malaysia, Nilai.
iii. Perpustakaan Universiti Kebangsaan Malaysia, Bangi.
iv. Perpustakaan Awam Pusat Islam, Kuala Lumpur.

This research can possibly judge its reliability and validity of study because it is base on the theory of laws within the actual scenario in related cases had reported in law journals. Besides the reviewing definition and other important aspect of computer crime, the method of comparison, incrimination and investigation will be held in this research process. The ethical of research and other procedure will be taking in consideration towards produce the neat and pure research that may replicate by other research.

Using the library-based method, here will be no questionnaire will be conducted but some interview may take part as the additional sources to get the various ideas. The data that collected from library and Internet will be analyzed through comparisons and the differences which arise through various situation, consideration and the art of judgment with the decision that made by the laws practitioner either honestly using the authority had given or by the concept of manipulation.

The author also uses the documentation method. It is one of the ways which was using by the author to collect the data and information that was printed. These are the most way used by the author. The author referred the books and article to get the information.

Beside of that, the author also referred the other reference such as thesis, journal, magazine, newspaper and others. Such things are very useful to the author to complete this research. With these references, the author can get more data and information that can give first clear view about the topic of the research.

CHAPTER TWO

CHAPTER TWO

COMPUTER CRIME UNDER MALAYSIAN LAW

2.1 Definition

2.1.1 Definition of Computer

There are several definitions which can be used to define the meaning of computer. The definition can be taken in many sources like dictionary, books and other material.

Based to the Federal Chambers Advanced English Dictionary, the computer can be defined as an electronic machine that stores large amounts of information, or a similar machine that can be made to control some mechanical operation[1].

Syariah Court Evidence (Selangor), describes computer as any device for recording, storing, processing, retrieving or producing any information or other matter, or for performing any one or more of those functions, by what ever name or description such device is called; and where two or more computers carry out any one or more of those functions in combination or in succession or otherwise howsoever conjointly, they shall be treated as a single computer[2].

The computer crime can be described as any illegal act that involves a computer, its system or its application. It is any intentional act associated in any way with computers where a victim suffered or could have suffered a loss and a perpetrator made or could have made or could have made a gain[3].

---

[1] *Federal Chambers Advanced English Dictionary*. 2002. Federal Publication Sdn. Bhd. Fourth Print
[2] Malaysia. 2005. *Syariah Court Evidence* (Revised 2005). (Enactment 2003). Section 3.
[3] Gerald L. Ferrera. *Cyber Law; Text and Case.* West Thompson Learning: Australia. p.300

The United States Department of Justice provided that computer crime is any illegal act for which knowledge of computer technology is essential for its perpetration, investigation and prosecution[4].

According to the Computer Crime Act 1997, the computer means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility[5].

The computer also can be defined the computer must be a device which posses certain characteristics such as it can be an electronic device, a magnetic device and others[6].

2.1.2 Definition of Computer Crime

There are various definitions relating to computer crime. Firstly, the computer crime can be defined as crime related to the information technology, electronics commerce and others[7].

The other definition is said that computer crime is a breaking the criminal law by use of a computer[8], such as fraud, stealing data, spread the viruses, use the pirate product and others. A Computer Crime also is a crime committed with the aid of, or directly

---

[4] Gerald L. Ferrera. *Cyber Law; Text and Case.* p.300
[5] Malaysia. 2000. *Computer Crime Act 1997* (Revised 2000). (Act 563). Section 2(1).
[6] Julian Ding. 1999. *E-Commerce Law and Practice.* Sweet and Maxwell Asia: Petaling Jaya. p. 264.
[7] R. K. Suri. 2001. *Information Technology Laws.* International Law Book Service: Kuala Lumpur. p. 325.
[8] http://computing-dictionary.thefreedictionary.com/computer%20crime

involving, a data processing system or network[9]. A crime committed using a computer or data stored on a computer[10].

Computer crime referring to abuse computer equipment provide damage, stealing or change inner data computer. Computer crime difficult to be proven or detected caused loss of data or reproduction data happened like virtual and unable to be proved physically[11].

2.2 The Role of Computers in Crime

2.2.1 Type of the Computer Crime

There are many types of computer crime that exists nowadays in Malaysia and also in the world. This type of computer crime can be divided into four big types which concise many type of it. The crime can be named as[12]:

a) Breached of Physical Security
b) Breached of Personnel Security
c) Breached of Communication and Data Security
d) Breached of Operations Security

---

[9] http://www.legalmountain.com/Legal%20Topics/Computer%20Crimes.htm
[9] http://computeruser.com/resources/dictionary/definition.html?lookup=1654

[10] David Icove, Karl Seger & William Von Storch. 1995. *Computer Crime A Crimefighter's Handbook.* Online Catalog.

[11] http://www.jawab.com.my/Jenayah-komputer

Breaches of Physical Security

Physical security is concerned with physical protection of the computer, computer equipment, computer media, and the overall physical facility from natural disasters, accidents of various kinds, and intentional attacks. That chapter describes the basics of what is being protected, and provides guidelines that will help keep your facility physically secure.

The simple examples of breaches of physical security are like the terrorist bombings on buildings housing computer equipment, arson, and theft and destruction of computer equipment fall into this category. You may not realize that less obvious attacks, like turning off the electricity in a computer room, spilling soda on a keyboard, and throwing sensitive papers in the trash may also invite disaster. This section describes some of these less obvious breaches.

Dumpster Diving

Dumpster diving or trashing, is a name given to a very simple type of security attack. It also can be described as scavenging through materials that have been thrown away. The figure one (1) in the appendix A can show this situation. This type of attack is not illegal in any obvious way. If papers are thrown away, nobody wants them. Dumpster diving also is not unique to computer facilities. All kinds of sensitive information turn up in the trash, and industrial spies through the years have used this method to get information about their competitors.

Computer facilities are especially good places for scavengers who are looking around for information that might help them penetrate a system. Around the offices and in the trash, crackers can find used disks and tapes, discarded printouts and handwritten notes of all kinds. Crackers have been known to literally dive into the dumpsters outside telephone companies and network providers, searching for passwords and access codes. They may also retrieve printouts, computer manuals and other documents from which they extract

information needed to crack the system. The trash of computer and telephone companies is of special interest to trashes because it is usually a rich source of helpful information. There is another type of computer-related trash that might not consider. In the system itself are files that have been deleted, but that have not actually been erased from the system. Computers and computer operators are oriented towards saving data, not destroying it. Sometimes data is saved that should not be. Remember the last time the system crashed while was working on a project. Even though you might have lost some data, the person still probably able to recover using a backup that he or the system operator or administrator made.

Electronic trashing is easy because of the way that systems typically delete data. Usually, "deleting" a file, a disk, or a tape does not actually delete data, but simply rewrites a header record. If you are running MS-DOS, for example, you can delete a file via the "DEL" command. However, someone can retrieve the contents of the file simply by running "UNDELETE". System utilities are available that make it easy to retrieve files that may seem to be completely gone.

Although there are methods for truly erasing files and magnetic media, most computer operators who work on large systems do not take the time to erase disks and tapes when they are finished with them. They may discard old disks and tapes with data still on them.

They simply write the new data over the old data already on the tape. Because the new data may not be the same length as the old, there may be sensitive data left for those skilled enough to find it. It is far safer to explicitly write over storage media and memory contents with random data and to degauss magnetic tapes.

Wiretapping

There are a number of ways that physical methods can breach networks and communications. Some of the offenses will discuss under the topic of "Breaches of Communications Security," later in this chapter. Telephone and network wiring is often

not protected as well as it should be, both from intruders who can physically damage it and from wiretaps that can pick up the data flowing across the wires.
Criminals sometimes use wiretapping methods to eavesdrop on communications. It is unfortunately quite easy to tap many types of network cabling. For example, a simple induction loop coiled around a terminal wire can pick up most voice and RS232 communications. More complex types of eavesdropping can be set up as well. It is important to physically secure all networks cabling to protect it both from interception and from vandalism.

Telephone fraud has always been a problem among crackers, but with the increasing use of cellular phones, phone calling cards, and the ordering of merchandise over the phone using credit cards, this problem has increased dramatically in recent years.

Denial or Degradation of Service

A few security breaches span most of the categories discussed in this topic. How these breaches are categorized depends largely on the methods used to prevent or detect them. In security terms, availability means that the computer facility, the computer itself, and the software and data users need are all working and available for use. Someone who shuts down service or slows it to a snail's pace is committing an offense known as denial of service or degradation of service. There are many ways to disrupt service, including such physical means as arson or explosions; shutting off power, air conditioning, or water (needed by air conditioning systems); or performing various kinds of electromagnetic disturbances.

Actually, there are two quite different types of attacks in this category. Some cases of electronic sabotage involve the actual destruction or disabling of equipment or data. Turning off power or sending messages to system software telling it to stop processing are examples of the first type of attack, a classic denial of service.