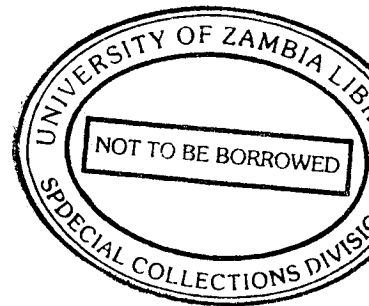


**COMPUTER CRIMES: ZAMBIA'S APPROACH TOWARDS THE  
DEVELOPMENT OF THE LAW IN COMPUTER CRIMES. IS THE LAW  
ADEQUATE IN ITS APPROACH TO THE DEVELOPMENT OF COMPUTER  
CRIMES?**



**BY**

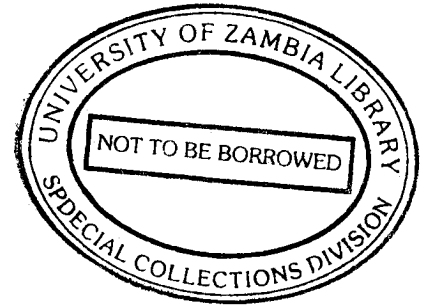
**MAPENZI .C. HAMACHILA**

**(20039336)**

**A PAPER SUBMITTED TO THE UNIVERSITY OF ZAMBIA IN THE PARTIAL  
FULFILMENT OF THE REQUIREMENT FOR A BACHELOR OF LAWS  
DEGREE, LL.B**

**NOVEMBER 2005**

**COMPUTER CRIMES: ZAMBIA'S APPROACH TOWARDS THE  
DEVELOPMENT OF THE LAW IN COMPUTER CRIMES. IS THE LAW  
ADEQUATE IN ITS APPROACH TO THE DEVELOPMENT OF COMPUTER  
CRIMES?**



**BY**

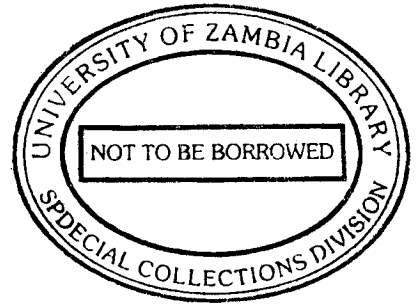
**MAPENZI .C. HAMACHILA**

**(20039336)**

**A PAPER SUBMITTED TO THE UNIVERSITY OF ZAMBIA IN THE PARTIAL  
FULFILMENT OF THE REQUIREMENT FOR A BACHELOR OF LAWS  
DEGREE, LL.B**

**NOVEMBER 2005**

**THE UNIVERSITY OF ZAMBIA  
SCHOOL OF LAW**



I RECOMMEND THAT THIS DIRECTED RESEARCH UNDER MY SUPERVISION

BY

**MAPENZI. C. HAMACHILA**

ENTITLED

**COMPUTER CRIMES: ZAMBIA'S APPROACH TOWARDS THE  
DEVELOPMENT OF THE LAW IN COMPUTER CRIMES. IS THE LAW  
ADEQUATE IN ITS APPROACH TO THE DEVELOPMENT OF COMPUTER  
CRIMES?**

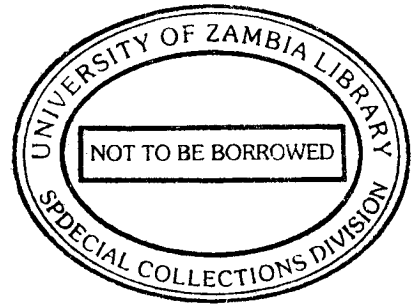
BE ACCEPTED FOR EXAMINATION. I HAVE CHECKED IT CAREFULLY AND I  
AM SATISFIED THAT IT FULFILS THE REQUIREMENTS IN RELATION TO THE  
FORMAT AS LAID DOWN IN THE REGULATIONS GOVERNING DIRECTED  
REASEARCH.

DATE 5<sup>th</sup> December 2005

SUPERVISOR

  
S.E. KULUSIKA

**THE UNIVERSITY OF ZAMBIA  
SCHOOL OF LAW**



I RECOMMEND THAT THIS DIRECTED RESEARCH UNDER MY SUPERVISION

BY

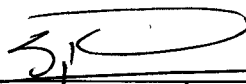
**MAPENZI. C. HAMACHILA**

ENTITLED

**COMPUTER CRIMES: ZAMBIA'S APPROACH TOWARDS THE  
DEVELOPMENT OF THE LAW IN COMPUTER CRIMES. IS THE LAW  
ADEQUATE IN ITS APPROACH TO THE DEVELOPMENT OF COMPUTER  
CRIMES?**

BE ACCEPTED FOR EXAMINATION. I HAVE CHECKED IT CAREFULLY AND I  
AM SATISFIED THAT IT FULFILS THE REQUIREMENTS IN RELATION TO THE  
FORMAT AS LAID DOWN IN THE REGULATIONS GOVERNING DIRECTED  
REASEARCH.

DATE 5<sup>th</sup> December 2005

SUPERVISOR   
S.E. KULUSIKA

## DECLARATION

I, Mapenzi. C. Hamachila, Computer Number: 20039336, do declare that I am the author of this essay entitled; Computer Crimes: Zambia's approach towards the development of the law in Computer Crimes. Is the law adequate in its approach to the development of Computer Crimes? I further solemnly declare that this work represents my own ideas and is not a production of any other work produced or submitted by any other person to the University of Zambia or to any other institution. Due acknowledgement has been given where other scholarly work has been cited.

Student's Name: ..... Mapenzi. C. Hamachila .....

Signature: ..... Hamachila. ....

Date: ..... 5<sup>th</sup> December, 2005 .....

## CONTENTS

	Page
Dedications.....	(i)
Acknowledgements.....	(ii)

### CHAPTER ONE

1.0 Introduction.....	1
1.1 Elements of The Crime.....	3
1.2 Incidence of Computer Crime.....	5
1.3 Penal Sanctions.....	10

### CHAPTER TWO

2.0 Introduction.....	12
2.1 Historical Background.....	12
2.1 (i) Computers In Workplace.....	15
2.1 (ii) Privacy and Anonymity.....	15
2.1 (iii) Intellectual Property.....	16
2.1 (iv) Professional Responsibility.....	17
2.1 (v) Computer Crime.....	18
2.1 (vi) Globalisation.....	19
2.2 Categories Of The Crime.....	20
2.2 (i) Breaches of Physical Security.....	20
2.2 (ii) Breaches Of Personnel Security.....	23
2.2 (iii) Breaches Of Communications and Data Security.....	24
2.2 (iv) Breaches Of Operation Security.....	26
2.3 Computer Crime In Other Countries.....	27
2.3 (i) United States of America.....	27
2.3 (ii) United Kingdom.....	28
2.3 (iii) Canada.....	30
2.3 (iv) Australia.....	30

CHAPTER THREE

3.0 Introduction.....32

3.1 Background To Computer Crimes In Zambia.....32

3.2 The Zambian Jurisdiction.....38

CHAPTER FOUR

4.0 Introduction.....44

4.1 Review of Computer Crimes.....44

4.2 Analysis.....50

4.3 Recommendations.....53

4.4 Conclusion.....53

BIBLIOGRAPHY.....55

STATUTES.....56

REFERNCES.....56

WEBSITES.....57

## **DEDICATIONS**

TO MY FAMILY: You have contributed to my success in ways you cannot imagine. For this I am forever grateful.

TO MY FRIENDS: You are always there for me. You are my second family.

TO YOU, SNIB CHABALA MUSONDA.



## **ACKNOWLEDGEMENTS**

This work would not be complete if I did not express my thanks to people who helped me put it together.

S.E. Kulusika, my supervisor, thank you for your assistance. Having been my lecturer and tutor in my studies in law. Your lessons were not in vain. I thank you for the knowledge obtained from your teachings.

To the officers in the Anti-fraud Unit Department at the Zambia Police Headquarters in Lusaka.

Namatanga and Oscar, we started our academic journey together, my prayer is that we all reach our desired destinations. Siyasiya, thank you for your unreserved honesty. Trust, someone I can count on. Manda, my roommate and friend. Thank you for the use of your computer.

To Snib Chabala Musonda. My friend, companion, chief editor... the list goes on. Thank you for your advice and encouragement towards the completion of my work.

My indebtedness is to GOD for giving me this privilege of coming this far in my life. For the gift of love and the gift of life. I pray that you keep on being my pillar of strength, a source of my inspiration.

# CHAPTER ONE

## **COMPUTER CRIMES: An analysis of the nature of the crime**

### **1.0 Introduction**

In the advancement of technology, there has been a new category of crime that has evolved. This new category of crime is referred to as Computer Crime. “Ordinarily a crime is a wrong which affects the security or well-being of the public generally so that the public has an interest in its suppression.”<sup>1</sup> This chapter will address the issue of Computer crimes focusing on the specific nature of the crime. It will consider the elements that are to be satisfied so as to establish this type of crime. Other relevant issues as to why an interest should be put in recognising this crime are also to be highlighted in the other sections of this chapter. This shall encompass the incidence of the crime and also the potential threat this type of crime poses to society. Finally, a look at the penal sanctions as derived from the various selected jurisdictions shall also be addressed.

Computer crimes are those unlawful interferences to the information that is stored in the Computer or any device that is used as an external store of information in a computer.<sup>2</sup> What is of relevance is that part of the computer known as ‘software’. “ Software is the term that is used to describe all different programs that may be used on a computer system. It also refers to the data that the programs process and the information that the

---

<sup>1</sup> Lord Hailsham, Halsbury’s Laws of England 4<sup>th</sup> Ed, Vol 11 London: Butterworths (1976) .p.11, para 1

<sup>2</sup> Icove, D et al. Computer Crimes: A Crime Fighter’s Handbook Texas: O’Reilly and Associates Inc. (1995) . (1.2) [http://www.oreilly.com/catalog/crime/chapter/crime\\_02.html](http://www.oreilly.com/catalog/crime/chapter/crime_02.html)

programs produce.”<sup>3</sup> It is that part of the Computer system that we cannot touch. The interference must be directed towards the software of the computer or any device used to store the software in which the information of the computer is stored. Therefore, any unlawful access or interference by those not privileged or having authority to the information that is stored on the computer constitutes what is known as Computer crime.

Any unlawful interference to the physical part of the Computer may be addressed legally by the provisions of the *Zambian Penal Code*.<sup>4</sup> The physical part of the computer is known as the ‘hardware’. “The hardware of a computer includes all components that one can touch and feel.”<sup>5</sup> It includes parts like the Monitor and the Keyboard. Division V of the *Penal Code* relates to Theft. This falls under section 264 which describes what is capable of being stolen and section 265 under the said Division defines what theft is. The definition is as follows;

*“A person who fraudulently and without claim of right takes anything capable of being stolen, or fraudulently converts to the use of any person other than the general or special owner thereof anything capable of being stolen, is said to steal that thing.”*

If an individual’s action in acquiring a Computer does so as provided for under section 265(1) of the *Penal code*, then the offence falls under theft.

The physical part of the Computer does not fall in the conventional category of Computer crimes. Computer crime is that part of Criminal law that addresses the untouchable part

---

<sup>3</sup> Libati, H.M. *Data Processing: Examination Questions And Answers*. Ndola: Mission Press. (2001) p.102

<sup>4</sup> CAP 87 Of the Laws Of Zambia

<sup>5</sup> Libati, H.M. *Data Processing: Examination Questions And Answers*. Ndola: Mission Press (2001) p.102

of the Computer. That part is called the 'software' of the Computer. It is this part of the Computer which is meant to be protected from unlawful access or interference by those not privileged or having authority to the information that is stored on the Computer.

This branch of criminal law has evolved to address a rather new aspect which has evolved in the 19<sup>th</sup> Century. "What the law has been trying to do is adjust relations and order conduct so as to give the most scheme of expectations of men in civilised society...".<sup>6</sup>

In today's world, Computer technology plays a major role in the social, political and economic aspects of the lives of the people. There has been a growing desire of the need to safeguard the exchange of information for the interests of the people concerned. It is a well known fact that if information falls in the wrong hands it can have some adverse effects. It is against this that it is necessary to have a look at the issue of computer crimes in a way that makes the whole aspect necessary for analysis.

### **1.1 Elements Of the Crime**

For a crime to be fully established as one, there must be certain elements that have to be satisfied. These elements are referred to as 'Actus reus' and 'Mens rea'. "If there was no

---

<sup>6</sup> Pound, R. Justice according To Law. London: Oxford University Press. (1976) p.131

*actus reus* or if the accused had no *mens rea* at the time that he caused the *actus reus* then the accused must be acquitted...”<sup>7</sup>

‘Actus rea’ refers to the illegal or unlawful commission or omission of the perpetrator in engaging in the commissioning of the offence. The commission or omission must be toward the commissioning of the offence, directly or indirectly. The “...actus reus may be so defined as to include acts of omission as well as acts of commission a person may incur criminal liability for failing to do that which the law prescribes.”<sup>8</sup> To constitute a Computer crime, the perpetrator must have had access or made efforts to have access to the information stored on the Computer or any relevant device. There should be actual infringement on the Computer or the device where the information is stored. This can be done in a number of ways. One such way is when one is in possession of an identity card used to have access to a Computer or the physical manipulation of the Computer to have access to the information.

The intention, which is blameworthy, is also a requisite component; “... a person is not to be made criminally liable for serious crime unless he intends to cause, or foresees that he will probably cause, or at the lowest, that he may cause, the elements which constitute the crime in question.”<sup>9</sup>

---

<sup>7</sup> Ian Mclean et al, Harris’s Criminal Law 22<sup>nd</sup> Ed. New Delhi: Universal Publishing Co Pvt Ltd. (2000) p.15

<sup>8</sup> Lord Hailsham, Halsbury’s Laws Of England 4<sup>th</sup> Ed Vol 11 London: Butterworths (1976) p.13, para 5

<sup>9</sup> Ibid (p.16, para 10)

Once the information is obtained, the perpetrator must have the intention to use the information in a way that is unlawful or detrimental to the ones who are the lawful possessors of such information. The perpetrator must have had a prior motive to gain some form of personal advantage by acquiring the particular information from the Computer or any other relevant device. Therefore, the intended use of the information should be illegal or unlawful and as such must be proved to be so. For example, Computer software piracy is primarily the obtaining of some advantage from a product without the authority of the initial producer of the software.<sup>10</sup>

## **1.2 Incidence of Computer Crime**

Knowledge on the topic of Computer crimes has received much attention in the western world or the American and European jurisdictions in particular. In these jurisdictions, much has been developed in relation to Computer crimes. A number of these crimes have been prosecuted each falling in a specific category. For example, "... one company in Texas that does business with a certain company asked them to mount a temporary storage (scratches) tape on the tape drive, the read-tape light would always come on before the write-tape. The ingenious oil company was scavenging the tape before information that might have been put on it by competitors that used the tape before them."<sup>11</sup>

---

<sup>10</sup> Icové et al., Computer Crimes: A Crime Fighter's Handbook. Texas: O'Reilly and Associates Inc (1995)  
[http://www.oreilly.com/catalog/crime/chapter/crime\\_02.html](http://www.oreilly.com/catalog/crime/chapter/crime_02.html)

<sup>11</sup> Ibid

This category of crime is perpetrated by those who wish to scavenge through the disposed trash of Computer and Telephone companies, as these are a rich source of information. Perpetrators obtain these discarded materials and strive to use the information on them which the original owners might have treated as trade secrets or kept as some form of confidential record. In these jurisdictions, much attention has been given to Computer crimes due to the fact that there has been a steady increase in the rate these crimes are committed.

In the recent past, different legal systems have been striving to find measures of adapting their legal systems to the new challenge of Computer crimes. From the statistics that have been gathered, the number of these cases that have been dealt with are on the rise. An example of a jurisdiction in which the aspect of Computer crimes has been separately and distinctly set up in the legal system is the American legal system.

These offences have been committed by individuals from all sectors of society. Perpetrators range from Juveniles, Employees and also those individuals known to be specialised in the field of Computer crimes. Below is a table comprising of some cases that have been prosecuted between the years 1998 and 2005. The table is just a sample of cases that have been recently prosecuted in the category of Computer crime cases in the United States of America. The offences committed comprised of a breach of Confidentiality (C), Integrity (I) and Availability (A) which are the interests alleged to have been breached.

Confidentiality breach is when a person knowingly accesses a computer without authorisation or exceeding authorisation access. Integrity occurs when a system or data has been accidentally or maliciously modified, altered or destroyed. Finally, Availability occurs when an authorised user of a Computer system is prevented from timely, reliable access. The following is table lists some of the cases that have been prosecuted in the United States of America jurisdiction. The following is table 1.1.<sup>12</sup>

Table 1.1

Computer Crime Chart Case	Interest Harmed	Target	Perpetrator Charged		Geo-graphy	Punishment		Other
Colloquial Case. Name (District) Press Release Date	Confi. (C) Integ. (I) Avail. (A)	Private, Public or Threat to Public Health or Safety	Juvenile	Group	Int'l	Sentence in Months	Fine	
US v Carlson (E.D Pa) July 11, 2005.	CA	Private				48		
US v Unnamed Juvenile (W.D Wash) Feb 11, 2005	IA	Private	X			18		Created RPCSDBOT variant of “blas worm.

<sup>12</sup> <http://www.usdoj.gov/criminal/cybercrime/cccases.html>



Confidentiality breach is when a person knowingly accesses a computer without authorisation or exceeding authorisation access. Integrity occurs when a system or data has been accidentally or maliciously modified, altered or destroyed. Finally, Availability occurs when an authorised user of a Computer system is prevented from timely, reliable access. The following is table lists some of the cases that have been prosecuted in the United States of America jurisdiction. The following is table 1.1.<sup>12</sup>

Table 1.1

Computer Crime Chart Case	Interest Harmed	Target	Perpetrator Charged		Geo-graphy	Punishment		Other
Colloquial Case. Name (District) Press Release Date	Confi. (C) Integ. (I) Avail. (A)	Private, Public or Threat to Public Health or Safety	Juvenile	Group	Int'l	Sentence in Months	Fine	
US v Carlson (E.D Pa) July 11, 2005.	CA	Private				48		
US v Unnamed Juvenile (W.D Wash) Feb 11, 2005	IA	Private	X			18		Created RPCSDBOT variant of “blasted worm.

<sup>12</sup> <http://www.usdoj.gov/criminal/cybercrime/cccases.html>

US v Salcedo et al (W.D.N.C) Dec 15, 2004	CI	Private		X		108		
US v Patterson (W.D.Pa) Dec 2, 2003.	CA	Private				18		Former Employee
US v Lloyd (D.N) Feb 19, 2002.	IA	Private				48	2M	Disgruntled Former Employee
US v Turner (N.D Ohio) Feb 19, 2002.	CIA	Public				12	199K	Employees (unauthorised) access credit ca account
US v Osowski (N.D.Ohio) Nov26,	CIA	Private				34	7.8M	Cisco accounta stole stoke fro company
US v Alibris (D.Mass) Nov 22, 1999.	C	Private				0	250K	Corporation
US v Unnamed Juvenile (D.Mass) March 18, 1998	CA	Threat to Public Health and Safety				TBD	TBD	FAA control tow disabled

From the table 1.1 above, it can be assessed that the number of cases on average involving computer crimes has been on the increase. The number of cases has been increasingly progressively, especially from the year 2001 to 2005. The previous table is only a summary of cases that have been prosecuted in the American courts. They involve

a range of perpetrators from Juveniles to corporations. Perpetrators of these offences are seen to pose a number of threats to society. They include private threats like theft, and public threats like disabling of control towers.

The table below illustrates the percentage rise of cases over the recent years in the American jurisdiction. Below is table 1.2.

Table 1.2

Year	Number of Cases	Type of Offence
2005 (as at present)	10%	CIA
2004	18%	CIA
2003	24%	CIA
2002	20%	CIA
2001	14%	CIA
2000	4%	CIA
1999	5%	CIA
1998	3%	CIA

From the above, the percentage of recently handled cases has been rising progressively raising a need to look into the issue of these crimes. The incidence of the crimes is on a

steady increase as can be inferred from the tables referred to. This in turn suggests a need for the law to find ways to adequately address this growing problem. Things that have to be considered are the development of a suitable legal system. These legal systems should have institutions which are to provide ways of crime detection, investigation and also, law enforcement.

### **1.3 Penal Sanctions Of The Crime**

Each category of the offence carries with it a different and separate penalty. Using the American system which has already been referred to, the penalty can either be imprisonment or the payment of a fine or both. The period of imprisonment can range from one month to as much as one hundred and eight months for similar offences committed on an international nature.<sup>13</sup>

In Malaysia, efforts to curb this new kind of offence have been made by way of passing legislation specifically addressing computer crimes. The Computer Crimes Act of 1997 was passed under the laws of Malaysia. Under part III of the Ancillary and General Provisions, section 9(2) gives the jurisdiction of the Act and says as follows;

*“..., this act shall apply if, the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent or with a computer in Malaysia at the material time.”*

---

<sup>13</sup> US v Salcedo et al (W.D.) Dec 15, 2004.

The Computer crimes Act is the primary statute that is used when handling cases of computer crimes in Malaysia and all sanctions for the offences under this Act are prescribed therein.

Under the American system the recent cases have been prosecuted under the Computer Crime Statute, 18 U.S.C Subsection 1030 of their Federal law.<sup>14</sup>

For an effective insight into the scope of computer crimes and ensuring that the perpetrators are properly prosecuted, the already referred to legal systems, the Malaysian and the American system have enacted statutes that are specific in their reference to computer crimes and also providing a suitable legal framework with defined offences and penalties.

---

<sup>14</sup> <http://www.usdoj.gov.criminal/cybercrime/cccases.html>

# **CHAPTER TWO**

## **Historical Background and A General Overview Of**

### **Computer Crimes**

#### **2.0 Introduction**

In the last chapter, the issue of computer crime was discussed, bringing to light the nature of the crime and also outlining reasons as to why there is particular need for an investigation into the topic. In this chapter, the discussion will go a step further, in that, the historical basis that lead to the evolution of what now is termed computer crime shall be analysed. Further, the specific crimes which fall in this category shall also be mentioned and explained so as to give an understanding of these crimes. There shall also be a case study of selected legal systems and how they perceive this new legal challenge and also what solutions they have come up with.

#### **2.1 Historical Background**

The introduction of the law of computer crimes in the sphere of Criminal law was in the early 1900s. The sophistication of computer technology lead to a few scholars come to a realisation that there is a potential threat to the way people might use these new devices.

In 1950, Weiner published a book entitled “ The Human Use of Human Beings”<sup>15</sup>. This book brought to light the potential dangers that might result as to the use of computers. It also led to other scholars like Parker to explain the concept of Computer ethics which has been used as a major basis for the historical development of computer crimes. Parker said, “... that when people entered the computer center they left their ethics at the door.”<sup>16</sup> Individual users of computer showed either ignorance of the issue of computer ethics or just plain disregard of these ethics.

For one to fully understand as to why computer crimes should be recognised, there should be shown an appreciation of exactly what computer ethics are. They form a very fundamental criteria for the legal foundation of computer crime

“The term ‘computer ethics’ is open to interpretations both broad and narrow. On the one hand, for example, computer ethics might be understood very narrowly as the effects of professional philosophers to apply traditional ethical theories like Utilitarianism, Kantianism, or virtue ethics to issues regarding the use of computer technology. On the other hand, it is possible to construe computer ethics in a very broad way to include, as well, standards of professional practice, codes of conduct, aspects of computer laws, public policy, corporate ethics--even certain topics in the sociology and psychology of computing.”<sup>17</sup>

---

<sup>15</sup> Weiner, N. The Human Use of Human Beings: Cybernetics and Society, Houghton. Mifflin.  
<http://plato.stanford.edu/entries/ethics.computer/>

<sup>16</sup> Ibid.

<sup>17</sup> [www.bynum.southernnet.edu](http://www.bynum.southernnet.edu)

For purposes of the subject matter of this chapter, the perspective which shall be taken shall be that as explained as the broad interpretation of computer ethics. When an individual tries to understand the basis of construing these practices as worthy of being called crimes, it is very important to see these crimes in a broad sense. Each particular type of crime touches on a specific area of computer ethics.

There has been a realisation that the use of computers in the various spheres of society whether it be commerce, education, information conveyance or just mere private use, this technology is subject to a number of uses and abuses. The threats posed to society are numerous and therefore, the historical evolution of the law in computer crime has not been automatic or rather mechanical.

Therefore, there have been some efforts made to adapt this concept of computer ethics to ensure that the users of this technology bear in mind that the technology they use as an instrument of achieving social ends is also an instrument to which ethical responsibilities accrue to.

“ In the mid 1970s, Walter Maner<sup>18</sup> ... began to use the term ‘computer ethics’ to refer to that field of inquiry dealing with ethical problems aggravated, transformed or created by computer technology.”<sup>19</sup> This scholar brought out the point that, in fact, though computers ease the lives of many people, there are some problems that come with them.

---

<sup>18</sup> Weiner, N. The Human Use Of Human Beings: Cybernetics And Society, Houghton. Mifflin.  
<http://plato.stanford.edu/entries/ethics/ethics.computer/>

<sup>19</sup> Johnson, D.G. Computer Ethics In The 21<sup>st</sup> Century. Rome: 1992. Key note address at the ETHI COMP 99 Conference.



For purposes of the subject matter of this chapter, the perspective which shall be taken shall be that as explained as the broad interpretation of computer ethics. When an individual tries to understand the basis of construing these practices as worthy of being called crimes, it is very important to see these crimes in a broad sense. Each particular type of crime touches on a specific area of computer ethics.

There has been a realisation that the use of computers in the various spheres of society whether it be commerce, education, information conveyance or just mere private use, this technology is subject to a number of uses and abuses. The threats posed to society are numerous and therefore, the historical evolution of the law in computer crime has not been automatic or rather mechanical.

Therefore, there have been some efforts made to adapt this concept of computer ethics to ensure that the users of this technology bear in mind that the technology they use as an instrument of achieving social ends is also an instrument to which ethical responsibilities accrue to.

“ In the mid 1970s, Walter Maner<sup>18</sup> ... began to use the term ‘computer ethics’ to refer to that field of inquiry dealing with ethical problems aggravated, transformed or created by computer technology.”<sup>19</sup> This scholar brought out the point that, in fact, though computers ease the lives of many people, there are some problems that come with them.

---

<sup>18</sup> Weiner, N. The Human Use Of Human Beings: Cybernetics And Society, Houghton. Mifflin. <http://plato.stanford.edu/entries/ethics/ethics.computer/>

<sup>19</sup> Johnson,D.G. Computer Ethics In The 21<sup>st</sup> Century. Rome: 1992. Key note address at the ETHI COMP 99 Conference.

A few areas have been selected to show just how these problems arise. These areas are not conclusively the only areas where ethical problems in computers arise.

(i) Computers In The Workplace

In work places, computers are being used or their use is extensively sought for in the never ending desire to improve on efficiency. This efficiency may reflect itself in forms of high profit margins or the ease with which work is now done. Therefore, "...even professionals like medical doctors, lawyers, teachers, accountants and psychologists are finding that computers can perform many of their traditional professional duties quite effectively."<sup>20</sup>

To preserve this, it is imperative that office workers should observe or adhere to their ethical obligations as regards to computer use. It is a fact that if an employee were to indulge in activities contrary to their responsibilities, such would jeopardise the work which they are supposed to do. And computers are one of the easiest ways in which one can commit a lot of offences in the work place. This brings one to seriously consider ways of ensuring that those who are found wanting are dealt with accordingly with the law.

(ii) Privacy And Anonymity

"The ease and efficiency with which computers and computer networks can be used to gather, store, search, compare, retrieve and share personal information make computer technology especially threatening to anyone who wishes to keep various kinds of

---

<sup>20</sup> Ibid

‘sensitive’ information (e.g. medical records) out of the public domain or out of the hands of those who are perceived as potential threats.”<sup>21</sup>

A lot of personal or confidential records are stored on many computer databases where easy and quick reference can be made. This type of record keeping is one most preferred because of many advantages it has as compared to hardcopy records. Large amounts of information can be stored through the use of computer technology as compared to other forms of record keeping.

Protection of these records becomes an aspect of vital concern because illegal access to the information or the records amounts to an inversion of the privacy of the owners of the records. The infringement on the privacy of an individual may pose as a great security risk and also may lead to some form of insecurity as to how secure ones private records really are from unlawful exposure to the public.

### (iii) Intellectual Property

“ One of the more controversial areas of computer ethics concerns the intellectual property rights connected with software ownership.”<sup>22</sup> Software ownership poses a very interesting challenge to the law. The major argument brought forward is that software-manufacturing companies have a right to enjoy the protection of their products from copying or duplication by others.

---

<sup>21</sup> Ibid (Article 3.1)

<sup>22</sup> Ibid (Article 3.4)

“ It is in Copyright law that demands for property rights in computer products have to date been most immediately satisfied. Something of that process has already been indicated in the general description of copyright law.”<sup>23</sup> A copyright is the way under Intellectual Property that computer software is protected from unlawful infringement by others. A copyright “..., is a right given against the copying of defined types of cultural, informational and entertainment productions.”<sup>24</sup> Software companies need to get something from their investment by way of some form of license and sales.

As a result of computer software copying, companies lose a lot of money. However it should be realised that software piracy is one offence that is quite difficult to curb. People do not think twice about copying a computer program for their personal use or just downloading a game from the Internet.

#### (iv) Professional Responsibility

There are people in society who are trained in the field of computers. These possess expertise in the use of computers and as such are given responsibilities in the field of computers by way of network installations or the development of new computer programs. “ Computer professionals have specialised knowledge and often have positions with authority and respect in the community.”<sup>25</sup>

---

<sup>23</sup> Cornish, W.R. Intellectual Property: Patents, Copyrights, Trade Marks And Allied Rights 3<sup>rd</sup> Ed. Delhi: Universal Publishing Co Pvt Ltd (2003) .p.441, para 13- 21

<sup>24</sup> Ibid. (p. 7, para 1-06)

<sup>25</sup> Johnson, Deborah.G. Computer Ethics in The 21<sup>st</sup> Century. Rome: A key-note address at the ETHI COMP Conference. 1999.

These computer professionals have a responsibility to other people so as not to compromise these relationships. The confidence entrusted in these people is high and any breach of this confidence brings down the whole concept of professional conduct necessary to maintain relations in the working environment. The following are the kinds of relations that are sought to be maintained: -

1. Employer - employee
2. Client – professional
3. Professional – professional
4. Society – professional

(v) Computer Crime

“ In this era of computer “viruses” and international spying by “hackers” who are thousands of miles away, it is clear that computer security is a topic of concern in the field of Computer Ethics. The problem is not so much the physical security of the Hardware (protecting it from theft, fire, flood, etc) but rather “ logical security”, which Sparfford, Heaphy and Ferbrache ( Spafford et al 1989 ) divide into five aspects;

1. Privacy and Confidentiality
2. Integrity – assuring that data and programs are not modified without proper authority.
3. Unimpaired service
4. Consistency – ensuring that the data and behaviour we see today will be the same tomorrow.
5. Controlling access to resources.”<sup>26</sup>

---

<sup>26</sup> Ibid

Computers have opened up new avenues to the perpetration of offences. Computer ethics encompasses computer crime to the extent that it is a major violation for the safeguard to the use of computers. Computer crime as earlier stated in chapter one, is concerned with the safeguard of the software of the computer and not the hardware in particular.

This aspect of computer ethics is on the increase as to need attention and is one that is more sophisticated as compared to other concerns of computer ethics. It is this aspect of computer ethics that forms the major topics of this chapter, the preceding and proceeding chapters. Computer crime is evolving everyday as progress is made in technological advancement in computer technology.

#### (vi) Globalisation

This refers to "... efforts to develop mutually agreed standards of conduct, and efforts to advance and defend human values, are being made in a truly global context."<sup>27</sup> The world is now referred to as a global village. There is interaction in many ways making the use of computers very important. Therefore, each member of this 'global village' should be able to protect its sovereignty and not be interfered by electronic means.

Standards should be set which are there to ensure that there is some protection afforded to computer users as well as other sectors of society that highly depend on computer technology in their operation. As earlier referred to, human values are an important component in the global context and thus need to be defended.

---

<sup>27</sup> Ibid (Article 3.6)

## **2.2 Categories Of Computer Crime**

Computer crimes fall into a number of categories. The following are some of the categories

1. Breaches of Physical security
2. Breaches of Personnel Security
3. Breaches of Communications and data Security
4. Breaches of Operations Security

### **2.2 (i) Breaches of Physical Security**

Breaches of physical security of computers is concerned with safeguarding the devices that are used to store information on the computer. External stores of information or data on a computer are also meant to be protected in this category of computer crime. The following are examples;

#### **a) Dumpster Diving**

Dumpster diving, or trashing, is a name given to a very simple type of security attack – scavenging through materials that have been thrown away. This type of security attack is not illegal in an obvious way.<sup>28</sup> This is because a lot of old materials are often disposed of if they are considered no longer useful to the users.

---

<sup>28</sup> Icové, et al. Computer Crime: A Crime fighter's Handbook 1<sup>st</sup> Ed. . Texas: O'Reilly And Associates Inc. (1995) ( Article 2.1). [http://www.oreilly.com/catalog/crime/chapter/crime\\_02.html](http://www.oreilly.com/catalog/crime/chapter/crime_02.html)

This, however, does not rule out the fact that sensitive information turns out in disposed off materials. There are also instances where an individual may write information which they should not printout or computer manuals. The major perpetrators of this type of offence are industrial spies or just foreign spies. These perpetrators go looking for information which they can use against the previous users of the discarded materials and thus there is need to protect the previous user from such violation of the data that might be stored on the devices.

It should be realised that in most computer devices, information though might be ‘erased’ or ‘deleted’, but is not so. Computer experts are able to find ways of retrieving information that may seem deleted to the usual user. The trash or disposed materials of Computer and Telephone companies are a rich source of information. This was earlier mentioned in Chapter one.

#### b) Wiretapping

“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 pick up the data flowing across the wires.”<sup>29</sup>

When it comes to wiretapping, criminals use special devices called wiretaps that they use to ‘eavesdrop’ on communications. This suggests a protection from interception or possible vandalism of network wiring from perpetrators.

---

<sup>29</sup> Ibid (2.2)



### c) Eavesdropping

Eavesdropping is a concern of military and intelligence data mainly. “ Computer equipment, like every other type of electrical equipment ..., emits electromagnetic impulses.”<sup>30</sup> These electronic emanations may be monitored, intercepted or dictated by perpetrators. This is done by both simple and highly sophisticated ways. An example of a simple case is the original Heath kit H19 terminals transmitted radio signals so strong they could be picked by placing an ordinary television set beside the terminals.

### d) Denial or Degradation of Service

The computer itself, the software and data users’ need should be all working and available for use. No one should stand in the way of a computer user and the computer either directly or indirectly. “Someone who shuts down service or slows it down to a Snail’s pace is committing an offence known as denial or degradation of service.”<sup>31</sup>

The physical means like arson or explosion shutting off power may lead to the disruption of the availability of the computer. This is done by way of electronic sabotage which is the actual destruction or disabling of equipment or data. An indirect way is the use of ‘ worms’ which are a kind of software which cause flooding or new processes to clog the affected system.

---

<sup>30</sup> Ibid (2.3)

<sup>31</sup> Ibid (2.4)

## 2.2 (ii) Breaches of Personnel Security

These breaches are laid down to protect those persons who are involved in the use or manufacture of the information that is either computer based or is in some way related to computer software. The following are some examples of breaches of personnel security.

### a) Masquerading

Masquerading is when one person uses the identity of another to gain access to a computer. This can be done personally or remotely. There are both physical and electronic forms of masquerading. An example of a physical form of masquerading is when one follows an authorised user and pretends to also belong to the authorised company and gains access to a computer. An electronic form is to use an authorised user's log-on identity card, password, personal identification number (PIN), or telephone access cord to gain access to a computer.

### b) Social Engineering

This occurs when someone manipulates others into revealing information that can be used to steal data or subvert systems. An example of this is when a person misrepresents himself or herself as to their identity and deceives others and thereby accessing information which is detrimental to other users.

### (a) Software Piracy

“Software piracy is an issue that spans the category boundaries and may be enforced in some organisations and not in others.”<sup>32</sup> This is so because, firstly, this offence is very difficult to curb and mostly noticed when it is perpetrated on a large scale. Those who copy software for private use seem to escape prosecution and therefore, the perpetration of the crime continues. “Too many people do not take copyrights seriously. Law abiding people everywhere think nothing of copying games to share with friends or office software for home use.”<sup>33</sup>

### 2.2 (iii) Breaches Of Communication and Data

This refers to attacks on the software itself and the data. It can be by way of inference and leakage.

#### a) Data Attacks

There are many types of attacks on the confidentiality, integrity and availability of data. The concepts of confidentiality, integrity and availability of data have already been explained in Chapter One.<sup>34</sup>

---

<sup>32</sup> Ibid (3.4)

<sup>33</sup> Ibid (3.5)

<sup>34</sup> Chapter One, (p.6)

Software piracy and the aspect of copyright intrinsically fall under data attacks. This is comprised in the unauthorised copying of data and the law of copyright provides protection of the owner or manufacturer of the software concerned.

Traffic analysis is an interesting but not obvious way of attacks on information or data. Even data that appears quite ordinary may be valuable to a foreign or industrial spy. The fact that two people are communicating -- never mind what they are saying to each other -- may give away a secret.<sup>35</sup> This is difficult to curtail but nevertheless a very important security concern.

Finally, a clever insider can hide stolen data in otherwise innocent output. This may be by way of a password launch code, or the location of sensitive information might be conveyed in this way.

#### a) Software Attacks

A session hijacking is when someone lurking nearby, probably a co- worker, who is not authorised to use the particular system, sits down to read or change files that he would not ordinarily be able to access. This may look simple but is one way in which computer data is interfered with and is easily violated. It may not be easy to detect the infringement unless the perpetrator is caught there and then when the offence is being committed.

The usual form of software attack, by way of introducing foreign software into the computer system, will inevitably distort the information on the computer. 'Trojan horses',

---

<sup>35</sup> Ibid (4.2)

‘computer viruses’ and ‘worms’ are examples of attacks that aim at the integrity of the data that is stored in a system and is communicated across network.

Trojan horses are computer programs that may lie dormant, in a way, in a computer system and only become effective when a suitable condition presents itself and then this program corrupts all the data that may be on the files.

A ‘virus’, also a computer program, has a characteristic of multiplying itself in a computer system by way of copying itself. It does so until it clogs the system and eventually corrupts the files or data on the computer. Finally, there are ‘worms’. These have a special characteristic of being able to move from one computer system to another. They too, like the ‘Trojan horse’ and computer ‘virus’, have a devastating effect on the system of the computer.

## 2.2 (iv) Breaches of Operations Security

Breaches on operations security mainly focus on finding ways of ensuring that all methods of attacks on the data on a system or personnel are detected.

### (a) Data Diddling

This basically involves the entry of false data onto a system of a computer. This in itself has serious consequences. It can lead to distortions of vital information that may be

stored on a computer system. Such kinds of modifications should be guarded against at all costs.

### **2.3 Computer Crime In Other Countries**

When faced with how to handle computer crimes a few countries have been selected and analysed to see how they have reacted to this issue. The following are the selected countries whose laws have been analysed. The initial analysis was done in a paper prepared by Michael. W. Kim on ethics and Law on the Electronic Frontier.<sup>36</sup>

#### **(i) United States of America**

The United States of America (USA) is one country in which the first important landmark statute in the field of computer crime was enacted. “In 1986, the passage of the Electronic Communications Privacy Act, marked the first time a major piece of legislation and specifically been passed to mandate restrictions on the use of computer.”<sup>37</sup>

This was the first time any governmental authority had done anything to try to contain what is now known as the Internet. The passage of the Electronic Communications Privacy Act laid a foundation to other forms of legislation.

---

<sup>36</sup> Paper for MT6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1997.  
<http://www.swiss.ai.mit.edu/6.805/student-papers/fall97-papers/kim-crime.html>

<sup>37</sup> Ibid

The Federal Bureau of Investigations (FBI) has established a network of Computer Crime Squads to curb the incidence of computer crime. The Justice Department has set up a set of guidelines outlining procedures for seizing and searching computers.

Another very significant thing is that the US population is now more educated about Computer Crime. There is enough literature available for them to learn of ways of protecting themselves and also fighting these crimes.

(ii) United Kingdom

“ On June 4, 1993, Neil Woods and Karl Struckland, citizens of the United Kingdom, became the first two people to be convicted and sentenced for violating the Criminal Conspiracy provision of the British Misuse Act of 1990.”<sup>38</sup> The two had been very dangerous hackers in Europe who were capable of penetrating Computer systems in fifteen countries. There had been another previous case involving one Paul Bedworth that ended in an acquittal. Though he had been found to have ‘hacked’ into a number of systems he was acquitted. Therefore, the Woods and Struckland case became a landmark case in the United Kingdom.

Two pieces of legislation were passed in relation to Computer Crimes. These were the Data Protection Act of 1984 and the Computer Misuse Act of 1990. The first Act was mainly concerned with the actual procurement and the use of the personal data on the computer. The second Act provided for laws, procedures and penalties surrounding unauthorised entry of individuals into computers.

---

<sup>38</sup> Ibid

The Data Protection Act of 1984 can be divided into eight basic principles. The first deals with procurement of data. It outlines ways in which data may be processed fairly and lawfully. The second is on processing of data. The data should be held in a specified and lawful manner for a specific purpose. This means that there should be special ways of storing the data depending on its nature. The third principle emphasises that data will not be used except for its intended purpose. Any other use will constitute a serious violation. The fourth stipulates that once the purpose for which the data is meant is finished, it should be disposed of immediately. The next two principles refer to integrity of data and that it should be kept accurate and up to date. The last two are on actual ownership of data and adequate security ensuring measures are taken to prevent its unauthorised access.

This Act is quite a controversial piece of legislation in that it seemed to protect the perpetrator instead of the victim. An example would be that if a victim of the offence had not taken steps to put measures to prevent any unauthorised access he would be found with a case to answer.

Due to this anomaly, the British Parliament passed the Computer Misuse Act of 1990<sup>39</sup>. This Act grew out of public outrage over the growing number of destructive ‘hackers’. In its construction, the first eighteen sections shifted the blame from the attacked to the attacker. Aspects like access, modification and destruction of material were now criminalised actions. The burden of intent in order to find one guilty was removed such

---

<sup>39</sup> Ibid



that if one gained illegal access to a system unconsciously, he was still guilty of an offence.

The remaining six sections of the Act defined the jurisdiction of the Act. Therefore, a case in 1995, involving one Christopher Pile, who was sentenced to eighteen months in prison for violating section 3 of the Computer Misuse Act was recorded.

#### (iv) Canada

In the Canadian legal system, there are basically two sections in the Canadian Criminal Code, section 342.1 and section 430 that deal with computer crimes. Section 342 has two parts:

- a) Items traditionally to be considered computer crime.
- b) Defines data or computer programs, to give written documents of what materials qualify under the statute.

Section 430 criminalises the actual destruction, alteration or interruption of data transmission. In Canada, there is a clear jurisdictional boundary for computer crime in the legislation present.

#### (v) Australia

In 1991, there was the passage of the Telecommunications Act, which basically added sections 74 and 76 to the Australian Criminal Code. Section 74 outlines the definition of 'carrier' and 'data', so that they may be used in subsequent sections of the code. It also

went further to specify what was considered a carrier and data belonging to the commonwealth of Australia.<sup>40</sup>

Following this, in 1993, an agency known as the Australian Federal Police was established. This was established only for the purpose of enforcing the Telecommunications Act.

Therefore, as can be inferred from above, countries have striven to take steps so as to find ways of curbing this crime. The significant step has been introducing specific legislations which are independent and specifically address the issue of computer crimes. The second step has been to bring in security agencies that are there to enforce these statutory enactments.

---

<sup>40</sup> Ibid

## **CHAPTER THREE**

### **Computer Crimes: The Zambian Perspective**

#### **3.0 Introduction**

This chapter is to consider the extent to which the Zambian criminal law has endeavoured to address this concept of computer crimes. In this line of approach, the statutory framework that has been set up shall be considered. This also means that a background of the present law as applied in Zambia shall be analysed. This will eventually lead to a study of the prevailing Zambian law and its enforcement.

#### **3.1 Background To Computer Crimes In Zambia**

The law on computer crimes in Zambia has its basis on the outcome of the Convention on Cyber-crime that was held in Europe<sup>41</sup>. The Convention and its Explanatory Report have been adopted by the Committee of Ministers of the Council of Europe at its 109<sup>th</sup> session (8 November 2001) and the Convention has been opened for signature in Budapest, on 23 November 2001, on the issue of the International Conference on Cyber-crime.<sup>42</sup>

It was at this International Conference on Cyber-crime that this broad issue was addressed at international level. In 1996, before the convention was adopted, the European Committee on Crime Problems decided in November 1996 to set up a

---

<sup>41</sup> Convention On Cybercrime: European Treaty Series- No 185 Budapest, 23.XI.2001

<sup>42</sup> Convention on Cybercrime (Explanatory Report)

Committee of Experts to deal with Cyber-crime. This Committee of Experts went round and gathered information related to Cyber-crime. The major driving force of the investigation is that the category of Cyber-space offences are either committed against the integrity, availability, and confidentiality of computer systems and telecommunications networks.

At the International Conference on Cyber-crime, issues that were raised included technical measures to protect computer systems that need to be implemented concomitantly with legal measures to prevent and deter criminal behaviour. Secondly, solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The Convention on Cyber-crime is one such international legal instrument. The present Convention aims to meet this challenge, with due respect to human rights in the new information society.

The Convention on Cyber-crime has three aims and they are, namely:

- a) *harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of Cyber-crime*
- b) *Providing for domestic criminal procedural law powers necessary for the Investigation and prosecution of such offences committed by means of A computer system or evidence in relation to which is in electronic form.*
- c) *setting up a fast and effective regime of international co-operation.*<sup>43</sup>

---

<sup>43</sup> Ibid

The first aim of the Convention highlights the need for countries to find ways of including provisions in the area of computer crime into their domestic criminal law. Each individual country should find the best-suited way of modifying its substantive law so as to incorporate computer crimes into the legal system. Jurisdictional variations are being considered here and no general imposition of any standard is being effected on any country.

Section 1 of the Convention refers to the substantive law issues. It defines nine offences that are grouped into four categories. The offences are,

- a) Illegal access
- b) Illegal interception
- c) Data interception
- d) System interference
- e) Misuse of devices
- f) Computer-related forgery
- g) Computer-related fraud
- h) Offences related to child pornography
- i) Offences related to copyright and neighbouring rights

Article 12 of the Convention relates to corporate liability, which incorporate corporations in the range of offences. All offences contained in the Convention must be committed “intentionally” for criminal liability to apply.<sup>44</sup> The exact meaning of “intentionally” should be left to national interpretation. Articles 2-13 of the Convention provide for ways

---

<sup>44</sup> Convention On Cybercrime (para, 39)

to improve the means to prevent and suppress computer, or computer related crime by establishing a common minimum standard of relevant offences.

Secondly, the Convention offers a guide that a signatory may adopt so as to ensure that the proper mechanism is enforced for the implementation of the law. “ Each State Party is obliged to adopt such legislative and other measures as may be necessary in accordance with its domestic law and legal framework, to establish the powers and procedures described in this section for the purpose of “ specific criminal investigations or proceedings”.”<sup>45</sup>

Article 21 of the Convention provides for exceptions or reservations that a State Party may enter. Article 21 specifically refers to the power to intercept ‘content data’ shall be limited to a range of serious offences to be determinable by domestic law. Secondly, that a party may reserve the right to apply the measures in Article 20 (real time collection of traffic data) only to offences or categories of offences specified in the reservation provided the range of offences to which it applies has the interception measures referred to in Article 21.

Procedural aspects that have been provided for in the Convention can be found in Article 18 and 19, which refer to a Production Order and the seizure of stored computer data respectively. Article 18 of the convention reads as follows:

---

<sup>45</sup> Ibid, (Para 141)

*Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:*

- a a person in its territory to submit specified computer data in that person's possession or control, which is stored in computer system or a computer data storage medium; and*
- b a service provider offering its service in the territory of the Party to submit subscriber information to such services in that service provider's possession or control.*

This Article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data. This enables the relevant authorities to have access to the prosecution of the data involved in the prosecution of the offence. The State Party may provide for a mechanism to compel an individual in possession of a computer in the event of an occasion requiring such.

The aim of Article 19 of the Convention is to establishing an equivalent power relating to stored data.<sup>46</sup> This Article refers to the search and seizure of computer data. There are variations in how stored computer data is referred to in various jurisdictions. Some jurisdictions do not consider computer data as 'tangible' objects and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects.<sup>47</sup> Therefore, there are some modifications in relation to how it may be

---

<sup>46</sup> Convention On Cybercrime (Explanatory Report) P.33, para 184

<sup>47</sup> Ibid.

made possible for authorities to have access to the stored computer data and conduct an effective search.

A third inclusion to the procedural part of the Convention relates to international co-operation of the State Parties. This is to be provided for under Article 22 of the Convention on Cyber-crime. Initially, the Article makes clear that international co-operation is to be provided among Parties “to the widest extent possible”.<sup>48</sup> State Parties are to provide extensive co-operation to each other.

The general scope of the obligation to co-operate is set forth in Article 23. Co-operation is to be extended to all criminal offences related to computer systems and data (i.e. offences covered in Article 13 paragraph 2 litterae a-b) as well as to the collection of evidence in electronic form of a criminal offence.<sup>49</sup> Finally, co-operation is to be carried out both “in accordance with the provisions of this chapter” and “through applications of relevant international agreements agreed to on the basis of uniform or reciprocal legislation and domestic laws.”<sup>50</sup>

State parties to the Conventions are obliged to provide international assistance to other State Parties. The obligation is not given any standard criteria, as it is expressed as to the ‘widest extent possible’. This, in itself, is subject to exceptions as to how far or to what extent the international co-operation will be effected. A consideration will have to be

---

<sup>48</sup> Convention On Cybercrime (Explanatory Report) (p.44, para242.)

<sup>49</sup> Ibid, (para 243)

<sup>50</sup> Ibid, (para 244)



given to the type of reciprocal legislation or domestic laws that are peculiar to the particular State Party or Parties.

The structure of the Convention is such that it is made of four chapters, namely:

- a) Use of terms
- b) Measures to be taken at domestic level-substantive law and procedural law
- c) International Co-operation
- d) Final Clauses

Zambia is a signatory of this Convention. Therefore, it is obliged to adhere to the Convention on Cyber-crime, which is still open for signing.

### **3.2 The Zambian Jurisdiction**

As earlier stated, Zambia is a signatory to the Convention on Cyber-crime. Based on the provisions of the said convention, there has been a piece of legislation, which has been passed in relation to Computer Crimes. The Act is known as The Computer Misuse And Crimes Act.<sup>51</sup> This Act was assented to on 2<sup>nd</sup> September 2004. The Act is divided into three parts, but our major concern will be parts II and III. Part II refers to offences under the Act and part III refers to general provisions. Part I refers to the preliminary section of the Act.

---

<sup>51</sup> The Computer Misuse And Crimes Act, No. 13 of 2004.

In the range of offences, the core offences of Confidentiality, Integrity and Availability have been addressed. Sections 4 and 5 deal with the aspect of confidentiality in terms of Computer Crimes. Section 4 of the Act particularly refers to unauthorised access to the computer program. Section 4 (1) reads:

*A person who knowingly and without authority causes a computer to perform any function for the purpose of securing access to any program held in that computer or any other computer commits an offence ... .*

Section 5 (1), which deals with access with intent to commit or facilitate commission of offence, states as follows:

*A person who knowingly causes the computer to perform any function for the purpose of securing access to any program or data held in that computer or any other computer with intent to commit or facilitate the commission of an offence involving property, fraud, dishonesty or which causes bodily harm, commits an offence ... .*

Sections 6, 7 and 9 of the Act deal with the aspect of Integrity. Sections 6 and 7 refer to unauthorised modifications of a computer program or data and unauthorised use or interception of computer service respectively. Section 9 refers to unauthorised disclosure of access code to gain access to any program or data held in a computer. The offences referred to are meant to protect the communications and the data that is on the computer and any other relevant device. According to section 6 of the Act, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.<sup>52</sup> What is of relevance is that there was some form of modifications undertaken. There is

---

<sup>52</sup> Computer Misuse And Crimes Act, No. 13 of 2004, s.6 (2) (b)

another provisio that pertains to section 7, which states that it is immaterial, that the unauthorised access or interception is not directed to any particular program or data of any kind or a program or data held in any particular computer.<sup>53</sup>

Sections 8, 12 and 13 of the Act deal with the aspect of Availability. The offences referred to here include unauthorised obstruction of use of computer, causing a computer to cease to function and omission to introduce, record or store data respectively. These types of offences as earlier stated in the preceding chapter,<sup>54</sup> relate to the available use of the computer to the authorised or lawful users of the computer.

Section 10 of the Act highlights a special feature of computers that are called “protected computers”. Section 10 (2) clearly explains what a protected computer is and reads as follows:

*..., a computer shall be treated as a “protected computer” if the person committing the offence knew, or ought reasonably to have known that the computer, program or data is used directly in connection with or is necessary for-*

- a) the security, defence or international relations of the state;*
- b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;*
- c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or key public infrastructure;*

---

<sup>53</sup> Ibid, s.7 (2) (a) (b) (c).

<sup>54</sup> Chapter One, (p.6)

- d) the storing of classified Government information, or*
- e) the protection of public safety and public health, including systems related to essential emergency services such as police, civil defence and medical services*

Any violation to protected computers carries with it a more serious penalty of a prison term not less than fifteen years but not exceeding twenty-five years or in lieu of penalties prescribed in sections four, five, six or eight, or to both. This line of offence seems to border on issues of national security.

Section 14 of the Act is a classic example of the adoption of one of the provisions in the Convention on Cyber-crimes. The provision referred to is Article 12 of the Convention, which refers to offences by body corporate. In this respect section 14 refers to offences by a body corporate. An interesting provision in this section, is that, if a corporation is convicted of an offence or fined, the director who is concerned in management of that corporation shall be deemed to have committed the same offence and is fined in person as if the person authorised or permitted the act or omission. An exception is where the offence was committed without the knowledge of the director or the director took reasonable steps to prevent the act from being committed.<sup>55</sup>

Part II of the Act refers to the substantive law as adopted in the Zambian jurisdiction in relation to Computer crimes. This is in line with Articles 2-3 of the Convention on Cyber-crimes that is addressed in chapter two of the Convention concerning substantive law issues.

---

<sup>55</sup> Ibid, s.14

Part III of the Computer Misuse And Crimes Act, Number 13 of 2004 relates to the procedural law as adopted from the provision of the Convention. Section 15 of the Act is a reflection of section 2 under Article 18 of the Convention, which refers to the provision of a 'Production Order'. In this respect, section 16 of the Act refers to search and seizure warrants.

This section empowers the authorities to have access to, inspect and check the operation of the computer. The seizure of computers, data, programs information or any document is to be effected if the authorities reasonably believe to be evidence that an offence under the Act has been, or is about to be committed.<sup>56</sup> Under the law, the warrant is issued by the Magistrate upon satisfaction by information on oath given by a police officer that there are reasonable grounds for believing that an offence under the Act has been or is about to be committed.<sup>57</sup>

From the above, it can be inferred that Part III of The Computer Misuse And Crimes Act, deals with the procedural aspects for the authorities to adhere, specifically section 16. Section 15 provides for an order for payment of compensation for any individual who is said to have suffered damage from the commission of the offence. Section 17 provides for regulations, which the Minister may, by statutory instrument make for the better carrying out of the provisions of the Act.

---

<sup>56</sup> Ibid, s.16 (3)

<sup>57</sup> Ibid, s.16 (1)

Part III of the Computer Misuse And Crimes Act, Number 13 of 2004 relates to the procedural law as adopted from the provision of the Convention. Section 15 of the Act is a reflection of section 2 under Article 18 of the Convention, which refers to the provision of a 'Production Order'. In this respect, section 16 of the Act refers to search and seizure warrants.

This section empowers the authorities to have access to, inspect and check the operation of the computer. The seizure of computers, data, programs information or any document is to be effected if the authorities reasonably believe to be evidence that an offence under the Act has been, or is about to be committed.<sup>56</sup> Under the law, the warrant is issued by the Magistrate upon satisfaction by information on oath given by a police officer that there are reasonable grounds for believing that an offence under the Act has been or is about to be committed.<sup>57</sup>

From the above, it can be inferred that Part III of The Computer Misuse And Crimes Act, deals with the procedural aspects for the authorities to adhere, specifically section 16. Section 15 provides for an order for payment of compensation for any individual who is said to have suffered damage from the commission of the offence. Section 17 provides for regulations, which the Minister may, by statutory instrument make for the better carrying out of the provisions of the Act.

---

<sup>56</sup> Ibid, s.16 (3)

<sup>57</sup> Ibid, s.16 (1)

Part III of the Computer Misuse And Crimes Act, Number 13 of 2004 relates to the procedural law as adopted from the provision of the Convention. Section 15 of the Act is a reflection of section 2 under Article 18 of the Convention, which refers to the provision of a 'Production Order'. In this respect, section 16 of the Act refers to search and seizure warrants.

This section empowers the authorities to have access to, inspect and check the operation of the computer. The seizure of computers, data, programs information or any document is to be effected if the authorities reasonably believe to be evidence that an offence under the Act has been, or is about to be committed.<sup>56</sup> Under the law, the warrant is issued by the Magistrate upon satisfaction by information on oath given by a police officer that there are reasonable grounds for believing that an offence under the Act has been or is about to be committed.<sup>57</sup>

From the above, it can be inferred that Part III of The Computer Misuse And Crimes Act, deals with the procedural aspects for the authorities to adhere, specifically section 16. Section 15 provides for an order for payment of compensation for any individual who is said to have suffered damage from the commission of the offence. Section 17 provides for regulations, which the Minister may, by statutory instrument make for the better carrying out of the provisions of the Act.

---

<sup>56</sup> Ibid, s.16 (3)

<sup>57</sup> Ibid, s.16 (1)

Therefore, as has been seen in this chapter, the provisions of The Computer Misuse And Crimes Act, Number 13 of 2004 are a reflection of the provisions of the Convention on Cyber-crime drawn in Budapest on 23<sup>rd</sup> November 2001. The model set up in the Convention has played a fundamental role in the legislative framework that has been established in Zambia to address this issue of Computer crimes.



## **CHAPTER FOUR**

### **Conclusion**

#### **4.0 Introduction**

The preceding chapters considered a number of issues pertaining to computer crimes, with special reference to Zambia. This chapter concludes discussion on the same by providing certain recommendations to enhance the fight against computer crimes in Zambia.

#### **4.1 Review Of Computer Crimes**

The origin of the whole concept of computer crimes is to be found in the concept of computer ethics. Computer ethics form a very important philosophical foundation to the law on computer crimes. As a new philosophy, computer ethics is one topic that an individual needs to fully understand to appreciate the reasons that are there to protect computers from unlawful interference. Aspects such as professional practice, codes of conduct, aspects of computer laws, public policy and corporate ethics<sup>58</sup> form the principle guidelines to lawful computer use.

There are a number of issues that are part of the scope of computer ethics. Some of those issues that have been considered include the issue of computer in the workplace. Work places have been targeted as one of the areas where the possibility and prevalence of

---

<sup>58</sup> [www.bynum.southernnet.edu](http://www.bynum.southernnet.edu)

computer violations is very high. There is need for professionals to be aware that though computers ease their work, there is an ethical responsibility that is attached to them. Protection of privacy of individuals is also a subject that is the concern of computer ethics. With a lot of people's confidential information being kept on computer databases, one can only find it necessary to protect those records from being accessed by unauthorised persons.

Computer crimes form the issues that are the subject matter of this discussion. As earlier stated, computer ethics in relation to computer crimes divides these crimes into five aspects, namely:

1. Privacy and confidentiality
2. Integrity- assuring that data and programs are not modified without proper authority.
3. Unimpaired service.
4. Consistency- ensuring that the data and behaviour we see today will be the same tomorrow.
5. Controlling access to resources.

Computer crime is one topic that stands to be seen as being aggravated and desires some form of immediate response.

To apply the principles of computer ethics, it is realised that the subject matter that is of need of protection is the software part of the computer. However, one category of

computer violations is very high. There is need for professionals to be aware that though computers ease their work, there is an ethical responsibility that is attached to them. Protection of privacy of individuals is also a subject that is the concern of computer ethics. With a lot of people's confidential information being kept on computer databases, one can only find it necessary to protect those records from being accessed by unauthorised persons.

Computer crimes form the issues that are the subject matter of this discussion. As earlier stated, computer ethics in relation to computer crimes divides these crimes into five aspects, namely:

1. Privacy and confidentiality
2. Integrity- assuring that data and programs are not modified without proper authority.
3. Unimpaired service.
4. Consistency- ensuring that the data and behaviour we see today will be the same tomorrow.
5. Controlling access to resources.

Computer crime is one topic that stands to be seen as being aggravated and desires some form of immediate response.

To apply the principles of computer ethics, it is realised that the subject matter that is of need of protection is the software part of the computer. However, one category of

computer crime that relates to breaches of physical security, in a way, safeguards that part of the computer hardware used for the external storing of data<sup>59</sup>. Eventually, it is the stored data that is in need of protection. The idea behind all this is that once the data that is on the computer is violated, there could be adverse consequences resulting from such a violation. For example, a notice was put up in one of the local Zambian newspapers talking of one Telecommunications Company having discovered that one of the competing mobile operators had installed gadgets on its direct exchange lines that had the effect of diverting calls meant for mobile phones from its switchboard<sup>60</sup>. This constitutes an offence that falls in the category of crimes known as breaches of physical security, to be specific, wiretapping. The end result is that the company stands to lose a lot of revenue from this violation.

The three main categories of computer crimes include Confidentiality, which refers to an instance when a person knowingly accesses a computer without authorisation or exceeds their authority. The second category is that of Integrity. Breach of Integrity occurs when a system or data has been accidentally or maliciously destroyed or modified. The last category is that of Availability. This is when the user of a computer is prevented from the timely use of the computer. It is from these three types of offences that other forms emanate from.

The other forms of offences that emanate from the three earlier mentioned categories of offences are as follows:

---

<sup>59</sup> Icove, et al. Computer Crimes: A Crime Fighter's Handbook 1<sup>st</sup> Ed. Texas: O'Reilly and Associates Inc (1995) [http://www.oreilly.com/catalog/crime/chapter/cr\\_02.html](http://www.oreilly.com/catalog/crime/chapter/cr_02.html)

<sup>60</sup> Saturday Post; No. 3285SA202- October 15, 2005. Page 4, " Malpractices On Zamtel Land Lines"

1. Breaches of Physical security
2. Breaches of Personnel security
3. Breaches of Communications and data security
4. Breaches of Operations security

The first types of offences, breaches of physical security, are offences concerned with safeguarding the devices used to store information on the computer. Areas of concern are illegal possession of such devices, intercepting the data flow from those devices and just impeding someone from having access to the information that is on the computer.

Breaches of Personnel security are offences against those who are involved in the use or manufacture of the information that is computer based or related to computer software.

Examples of these offences are masquerading, social engineering and software piracy.

The third type of offence, breaches of Communications and data, refer to attacks on the software itself and data. This can be achieved by way of interference or leakage. This involves the diversion of data by unauthorised means to some other location. This may be achieved by way of installing devices that are to tap from the mainstream flow of information that could be restricted. The final kind of offence refers to breach of Operations security. “Operation security includes the setting up of procedures to prevent and detect all type of attack on system and personnel,...”. A number of offences that fall into this category, like data diddling, consist of false data entry by way of modifying data before or after it is entered. Therefore, whatever action or omission that results in an

attack on the operation of a system of an organisation that results in some malpractice of the system falls into this category.

In the attempt to address this range of offences, different legal systems have put up measures to curb the perpetration of these offences. The United States of America, in its jurisdiction, is the first under which a statute was enacted so as to address computer crimes. This was done by way of the enactment of the Electronic communications Privacy Act of 1986. In addition to this, agencies were given the mandate to implement the Act one being the Federal Bureau of Investigations (FBI). These agencies have specialised personnel who are trained in the area of computer crimes. Other legal systems have in turn followed suit and also enacted their respective legislation.

In this respect, under the Zambian jurisdiction, there has been the enactment of the Computer Misuse and Crimes Act, number 13 of 2004. This piece of legislation is rather a new act and is barely just over a year old.

The model that was used to come up with this Act was that which was adopted at the Convention on Cyber crime in Budapest, Hungary on 23 November 2001. The Convention sets out the objects of the State Parties and also provides for some model for the members to follow in coming up with their own separate pieces of legislation. The Convention has three aims that attempt to address this whole issue of computer crimes.

Its first aim is harmonising the domestic criminal substantive law elements of offences related to computer crimes. Every country is allowed to look for ways of ensuring that the laws relating to computer crimes are compatible with the present domestic legal system. There is no imposition that is made on any particular country to comply with a certain legal model. The second aim of the convention applies to the procedural law to be adopted. This applies to areas such as investigation and prosecution of the offences. This is especially important because there is need to form new legal procedural rules as regards to things like the presentation and collection of electronic evidence depending on the particular crime.

The third and final aim relates to the issue of international co-operation. Computer crimes, due to their sophistication, are capable of being perpetrated outside one's own country. With the present day Internet age, individuals are capable of accessing databases that are hundreds of kilometers away from the confines of a computer room or any other computer. Therefore, there has been recognition under the convention that international assistance is vital to help prosecute perpetrators. In providing this co-operation among the state parties, a country is only obliged to provide it to the widest extent possible. There is no standard set up and a country can only co-operate only as far as it possibly can.

As earlier stated, the Computer Misuse and Crimes Act, is a relatively new piece of legislation. It has followed the model as provided for in the convention. In its structure, it has embodied provisions that provide for the address of the offences of Confidentiality, Integrity and Availability. This is in relation to the substantive law as to be provided for.

In relation to the procedural aspect, there is a provision laid down for the procuring of evidence. This is by way of powers that are given to the authorised officers who are to assist in the investigation of the offence. This is to be found in Part III of the Act.

#### **4.2 Analysis.**

At this point it is necessary to make reference back to the initial aim for this discussion on computer crimes. The major aim into this study is to find out exactly how far the law in relation to computer crimes has developed so far. Is the legal framework that has been adopted adequate in the development of a suitable legal response to the issue at hand?

The important response, which has been made under the Zambian jurisdiction, has been the enactment of the Computer Misuse and Crimes Act, number 13 of 2004. This is a positive development in the area of addressing the growing problem of computer crimes.

However, the Act does not clearly define what a computer crime really is. There is no provision for any explanation of what these crimes are. The Act is silent on this aspect. The Act merely quickly goes into the technicalities of the various kinds of offences. In its preamble, the Act reads,

*An Act to prohibit any unauthorised access, use or interference with a computer; to protect the integrity of computer systems and the confidentiality, integrity and availability of data; to prevent abuse of computer systems; to facilitate the*



*gathering and use of electronic evidence; and to provide for matters connected with or incidental to the foregoing.*

The Act merely outlines the various kinds of offences by making references to the ones of confidentiality, integrity and availability. It also makes reference to the procedural aspect of collection of evidence. It does not categorise these crimes so as to give one a clear understanding of their categorisation.

In terms of the scope of offences as to be found in the Act, it is quite comprehensive. Generally, all the areas of computer crimes have been addressed on a broad level. On the aspect of specific offences, three kinds have been provided for. These are, firstly, breaches of physical security. This is to be found in sections 7, 8 and 12 of the Act as unauthorised obstruction of use of computer. The second breach relates to personnel security as provided for in section 11 of the Act. The third is breach of communications and data security. This is in section 6 and could be committed by modifications to programs manually or by the introduction of other software such as computer viruses. Section 6 also provides for the fourth kind of offence that is breaches on operations security.

In the fight of computer crimes, the Convention on cyber crime makes reference to international co-operation that is to be to the widest extent possible. In the United States of American jurisdiction, section 2 of the USC. 18 of the Crimes and Criminal Procedures provides as follows,

(2) the term “protected computer” means a computer- -

(a) which is used in interstate or foreign commerce or communication, including

interstate or foreign commerce or communication of the United States;...

a computer located outside the United States that is used in a manner that affects

The above provision in particular applies to protected computers that fall in this category.

This is not what draws our interest in this case. What should be of interest is the point that in this statute, there is express application of a provision that applies to international co-operation. The section makes mention of the extent of the jurisdictional application of the Act.

In the *Zambian case*, there is no mention of any form of international co-operation in relation to the jurisdiction in the Act. The Act merely confines us to the *Zambian jurisdiction*. The only relief comes from the *Convention on Cyber-crime*. The inference is that only the signatories to the convention can provide such assistance and no other member.

Having a specific provision for international co-operation in curbing computer crimes in the Act has advantages. Firstly, the procedure of enforcement or extradition of information which might be cardinal to the cases is easily explained and understood. One does not have to go elsewhere for supporting legislation that may be used in the prosecution of offences. Therefore, the prosecution is made less complicated other than

bringing in issues that might lead to delay of the whole process. Secondly, the Act becomes more comprehensive in that it becomes wholly applicable and addresses all the relevant issues pertaining to computer crimes. The Zambian Act is lacking in these areas in the approach to computer crimes.

### **4.3 Recommendations**

The recommendations as to the provisions of the Act are as follows:

1. The Act should clearly define what a computer crime is.
2. The Act should categorise and explain the offences in the broad categories of Confidentiality, Integrity and Availability.
3. The aspect of international co-operation in relation to jurisdiction should be included in the Act.

### **4.4 Conclusion**

The law in its approach to the development of laws in computer crimes has taken a positive step. There has been no progressive approach in the development of any law that can be traced back to the evolution of the present Act. There is not much historical background in our Zambian situation to see any proper growth as the legal framework is just in its first stages of adopting and adapting laws to curb computer crimes.

bringing in issues that might lead to delay of the whole process. Secondly, the Act becomes more comprehensive in that it becomes wholly applicable and addresses all the relevant issues pertaining to computer crimes. The Zambian Act is lacking in these areas in the approach to computer crimes.

### **4.3 Recommendations**

The recommendations as to the provisions of the Act are as follows:

1. The Act should clearly define what a computer crime is.
2. The Act should categorise and explain the offences in the broad categories of Confidentiality, Integrity and Availability.
3. The aspect of international co-operation in relation to jurisdiction should be included in the Act.

### **4.4 Conclusion**

The law in its approach to the development of laws in computer crimes has taken a positive step. There has been no progressive approach in the development of any law that can be traced back to the evolution of the present Act. There is not much historical background in our Zambian situation to see any proper growth as the legal framework is just in its first stages of adopting and adapting laws to curb computer crimes.

The present Act, the Computer Misuse and Crimes Act, number 13 of 2004, is a good response to this issue. Though new, it has addressed all the major aspects of computer crimes as indicated in the discussion. There are only three issues that the Act has not dealt with adequately.

The first is the lack of a proper definition of what a computer crime is. All the Act has are examples of these crimes and their respective technicalities. Secondly, there is no proper categorisation of the various kinds of offences. Thirdly, there is a procedural deficiency in the Act in terms of international co-operation when prosecuting or investigating these crimes. Such a provision as exemplified in the American system is supposed to be expressed and provided for in the Act. Otherwise it brings in a void, which has to be filled by further introduction of other instruments.

The law in computer crimes is very new in the Zambian jurisdiction, and this suggests a need to provide some form of education to relevant agencies and other interested parties. As at present, the Anti-fraud Unit at the Zambia Police headquarters has taken up this responsibility of educating agencies and institutions in the area of computer crime. However, more is yet to be done to ensure success in this field.

## **BIBLIOGRAPHY**

Cornish, W. R. 2003. Intellectual Property: Patents, Copyrights, Trade Marks And Allied Rights, 3<sup>rd</sup> Ed. Delhi: Universal Law Publishing Co. Pvt. LTD

Icove David, Karl Seger and William Vornstorck. 1995. Computer Crimes: A Crime Fighter's Handbook, 1<sup>st</sup> Ed. Texas: O'Reilly and Associates Inc

Johnson, D.G. 1999. Computer Ethics In The 21<sup>st</sup> Century, a key-note address at the ETHI COMP 99 Conference, Rome, Italy, October 1999. Published In Spinello, Richard, A and Herman, T. Tavani, eds (2001). Readings In Cyber Ethics, Jones and Bartlett.

Johnson, D.G. 1992. Proprietary Rights In Computer Software: Individual and Policy Issues. In Bynum, Terrell Word, Walter Maner and John, L. Fodor eds. 1992. Software Ownership and Intellectual Property Rights, Research Center on Computer and Society.

Libati, H.M.2001. Data Processing: Examination Questions And Answers. Ndola: Mission Press

Lord Halsbury. 1976. Halsbury's Laws Of England, 4<sup>th</sup> Ed, Volume 11. London: Butterworths

McLean, Ian and Peter Morish.2000. Harris's Criminal Law 22<sup>nd</sup> Ed. New Delhi: Universal Publishing Co Pvt LTD

Pound, R. 1957. Justice According to Law. London: Oxford University Press

## **References**

- 1.The Convention On Cyber crime: European Treaty Series- No. 185 Budapest, 23.XI.2001
2. The Saturday Post; No. 3285SA202- October 15, 2005.

## **STATUTES**

1. The Computer Misuse And Crimes Act No. 13 of 2004.
2. Computer Misuse Act of 1990, of the Laws of England
3. Data Protection Act of 1984, of the Laws Of England
4. The Canadian Criminal Code
5. Electronic Communications Privacy Act of the Laws of the United States of America
6. Australian Criminal Code
7. The Telecommunications Act of Australia, Act of 1991.
8. The Penal Code, CAP 87 Of The Laws Of Zambia
9. Computer Crimes Act of 1997 Of The Laws Of Malaysia
10. Computer Crime Statute, 18 U.S.C. Federal Laws Of The United States of America
- 11.[www.bynum.southernnet.edu](http://www.bynum.southernnet.edu)
12. Computer Misuse Act of 1990,
13. Data Protection Act 1984,

14. The Canadian Criminal Code,

### **WEBSITES**

1. Bynum, Terrell, “ Computer Ethics: Basic Concepts and Historical Overview”, The Stanford Encyclopaedia of Philosophy (Winter 2001, Edition), Edward N. Zalta (ed), URL. <http://plato.stanford.edu/archive/win2001/entries/ethics-computer/>
2. Weiner, N. 1950/ 1954. The Human Use of Human Beings: Cybernetics and Society, Houghton, 1950. Houghton , Mifflin <http://plato.stanford.edu/entries/ethics/ethic-computer/>
3. [www.ktkm.gov.my/emplate01.asp?](http://www.ktkm.gov.my/emplate01.asp?)
4. <http://www.usdoj.gov/criminal/cybercrime/cccases.html>
5. Computer Misuse Act of 1990, <http://www.hmsso.gov.uk/acts/summary/0199018.html>
6. Data Protection Act 1984, <http://web.doc.ic.ac.uk/~ard/teach/DataProtectionAct.html>
7. The Canadian Criminal Code, <http://insight.mcmaster.ca/org/efa/pages/law/cc/cc.html>  
[www.bynum.southernnet.edu](http://www.bynum.southernnet.edu)
8. Icove David, Karl Seger and William Vornstorck. 1995. Computer Crimes: A Crime Fighter's Handbook, 1<sup>st</sup> Ed. Texas: O'Reilly and Associates Inc  
[http://www.oreilly.com/catalog/crime/chapter/cr\\_02.html](http://www.oreilly.com/catalog/crime/chapter/cr_02.html)