LAW RELATING TO COMPUTER CRIMES; IS IT EQUAL IN SRI LANKA AND UNITED KINGDOM?

A. S. Samarakoon *

History and Evolution of Computer

With the passage of time, social, cultural, economic and behavioral patterns of people Started to change and as a result, level of intelligence of people too started to improve and this made them to engage in experiments which further led innovations. These innovations introduced equipment with high technology and subsequently computers were made to meet challenges of the developing world.

Computers which were introduced as such were initially capable of performing minor tasks whereas now computers are developed to a greater level that those can perform tasks that an ordinary man cannot even think of doing. Computer was initially innovated by Greeks and as a result of its development, in 1812 Charles Babbage invented the abacus which performed the task of a computer. Computer was initially introduced for mathematical purposes. Later its purposes were widened and at present its technology has developed to a state where information of things happening around the world could be obtained in the doorstep of the user with the use of internet.

What are Computer Crimes?

Human beings in common have various qualities. They have certain qualities that come from birth. For an instance some human beings are introvert and others are extrovert. However behavioral patterns of human beings are a major determinant factor to analyze their qualities. Further morals and thinking patterns of people too act as an external factor in deciding these qualities and behavioral patterns. Thinking patterns of certain people could also be harmful when they do not consider about morals and societal norms. When people with such thinking patterns make use of technologically developed equipment such as computers in order to carry out their tasks, computer crimes take place.
National Institute of justice in United States of America defines computer crimes under three criteria[1]

1. Many persons are affected because of an act done with the use of knowledge on computer and technology by an individual or set of persons.
2.Using computers to commit crimes directly or indirectly relates to computer crime.
3.Any type of computer crime is wrongful under law relating to computer crimes.

Above three factors define the term computer crime clearly. According to first criteria, a computer crime has not been banned as an illegal act. For example,

* LLB (hons.)(KDU),
PGD in Criminology and Criminal Justice(USJ)

[1] Home office, accessed 9th April 2020 http://www.gov.uk/government/organizations/home-office>

ISSN 1800-055X Vol. Iv

murder is considered as an act which is banned by certain laws and regulations but computer crimes are not banned as such. Further only a handful of people have knowledge about computer crimes.

The specialty of computer crimes is that unlike other type of crimes; these have a characteristic of being subjected to change so rapidly. Because of that feature, when one such crime is identified by the authorities, another crime relating to the prior crime can take place at the same time. The main reason for that is computer crimes are directly influenced by technological advancement.

If a person intends to commit such a crime, he must possess the knowledge of handling a computer. The parties to a computer crime could be either one person or a set of persons. However, the effect of such crimes could be at times so serious that its damage cannot be calculated in monetary terms. For example, because of fraudulent activities that are done in banks using computers, both the bank and its customers are affected. Second criteria mention that computer must be used directly for a computer crime to take place. Which means a computer cannot function in isolation and it requires set of persons for it to be handled and controlled. Based on the nature of such an act a computer crime can take place. Third criteria define that these types of acts are wrongful under the laws that govern the state. Ex; Computer crimes act no 24 of 2007.

Crimes such as Cybercrime, Digital crime and High-tech crime must also be differentiated from computer crimes. At the same time, it is also important to identify the definitions presented on these type of crimes. Further according to Wikipedia, crimes that are widely done violating information technology related laws are termed as computer crimes.[2]

Internet is composed of a large number of websites. Crimes that are committed using internet are called internet crimes. It must be identified that there is a special criteria of requirements to identify a crime as a computer crime. For example, if a man injures another person by smashing with a computer, that would not come under the ambit of computer crime. Therefore, that shows that all the wrongful acts done using a computer would not fall under computer crimes. Therefore, as mentioned crime in order to be a computer crime must have unique features. However according to National Research Council Computer Report of 1991[3] , computer crimes which are committed using advanced technology, have a specific feature of spreading fast and can cause high damage could be more severe in the future than those crimes which are committed by using weapons and other dangerous weapons in the present. For example, when global positioning system is used for terrorist activities, more serious harm could happen than expected.

Therefore, computer crimes which are given different interpretations as provided above have become a serious

[2]Cybercrime, wikipediaorg accessed 10 April 2020 <https://en.wikipedia.org/wiki/cybercrime>

[3]computers at risk safe computing in the information Age, Napedu, accessed on 10th April 2020 <http://www.nap.edu/read/1581/chapter1>

issue and a threat to the current developing world. At initial stages only few crimes such as watching porn by children and spreading computer viruses were considered as computer crimes. However now the situation is so much changed that computer crimes take place along with the developing technology and one could hardly anticipate the effects caused by such crimes.

Computer crimes and related law in United Kingdom

It's been more than twenty years since first computer virus appeared. Since then such threats were influenced with the advancement of technology and were spread around the world along with the increasing number of computers being used. Until few years ago viruses and other malicious programs were mainly concerned as computer crime.

Most viruses were used to damage stored data and corrupt data in the hard disks. But now this has totally changed. At present, computer crime is a major issue which has extended to make illegal money. One of the major reasons for this change could be noted as the evolution of internet.

Computer crimes could take place either by computer being used as a tool to commit offence or by committing computer specific crimes. The case of ***Aids Information Trojan***[4] illustrates this point. In late 1989 this Trojan was distributed through a floppy disk by a company named PC Cybrog. The Trojan encrypted the contents of the hard disk and after ninety reboots leaving just a README file containing a PO Box address to which a payment was to be sent. However later the alleged author of the Trojan was extradited to United Kingdom to stand trial on charges of blackmailing and damaging computer systems.

The first legislation in United Kingdom which was designed to address computer crimes was "Computer Misuse Act of 1990". The Act mainly focused on the inadequacy of sufficient legal framework to deal with computer hackers. The Computer Misuse Act 1990 made provisions for securing computer material against unauthorized access or modification and for connected purposes which was set out under three computer misuse offences[5]

1. Unauthorized access to computer material
2. Unauthorized access with intent to commit or facilitate commission of further offences.
3. Unauthorized modification of computer material

Maximum prison sentences specified by the act for each of the above offence were six months, five years and five years respectively. However, amendment Computer Misuse act was introduced by "Police and justice Act 2006".

Section 02 of Computer misuse act 1990[6] holds that, a person is guilty of an offence

[4] *AIDS(Trojan horse)*, Wikipedia, viewed 10 th April 2020 <http://en.wikipedia.org/wiki/AIDS(Trojan_horse)>

[5] Computermisuse *Act 1990* , united kingdom, viewed 11 th April 2020 <http://www.legislation.gov.uk/ukpga/1990/18/contents

[6] ibid

ISSN 1800-055X Vol. Iv

if he commits an offence under section 01 (unauthorized access offence) with intent

a) To commit an offence to which this section applies or

b) To facilitate the commission of such an offence (whether by himself or by any other person)

In the case ***Ex parted***[7]**,** Allison was alleged to have obtained data relating to customer accounts which were false credit cards. This case related to application by United States authorities regarding securing unauthorized access to the American Express computer with the intent to commit theft and forgery. It was also alleged that the accused had caused unauthorized modification to the contents of the computer system. Following the decision in ***Bignall*** it was held that a section 1 offence had not been committed. On appeal the House of Lords rejected the notion that misuse of access rights could not incur criminal sanctions. Therefore, misuse of facilities by authorized users will expose them to the risk of criminal prosecution.

According to section 03 of computer misuse act 1990[8] a person is guilty of an offence if;

a) He does any act which causes an unauthorized modification of the contents of any computer

b) At the same time when he does the act he has the requisite intent and the requisite knowledge.

Section 03 requires that, performing of an act by accused which causes an unauthorized modification of contents of any computer and at the same time of commission of the act, the accused knew that any modification that he intended to cause is unauthorized. Further the accused intended either to damage the operation of any computer or prevent access to any data or program the computer or to impair the operation of any such program or the reliability of any such data.

Spam is also a serious issue faced by persons holding email accounts. Spam is also used to deliver malicious codes. Spam is the main tool of phishers to direct their victims to fake web sites from which confidential data is then taken. Having addressed to this issue, Department of Trade and Industry introduced the Privacy and Electronic Regulations (EC Directive) 2003.

The Police and Justice Act 2006 which covers broader issues than computer crime alone, also include amendments to the computer misuse act. Moreover, the prison sentence was increased up to two years from six months. Further section 3 of the Act relating to unauthorized modification of computer crime was amended to read unauthorized acts with intent to impair or with recklessness as to impairing operation

[7]***Regina v Bow Street Magistrates Court and Allison (AP) Ex Parte Government of the unitedstates of America*** (on appeal from a divisional court of the queen bench Division) viewed on 11 th April 2020 <http://www.publications.parliament.uk/pa/ld199899/ldjudgmt/id990805/bow.htm>

[8]*computer misuse act 1990*, united kingdom, <http://www.legislations.gov.uk/ukpga/1990/18/contents> accessed on 11 th April 2020

ISSN 1800-055X Vol. Iv

of computer and carries a maximum sentence of ten years[9].

It is a clear fact that existence of a specific legislation alone to govern criminal activities alone is not sufficient to overcome the issue of computer crimes. It is also required that authorities such as police must undertake a major duty in keeping up the lever of computer crimes at a lower level. Therefore, in order to overcome issues of computer crimes, the government of United Kingdom established the "National Hi-Tech Crime Unit" in year of 2001 with the objective of controlling computer crimes. However with the establishment of "Fraud act in 2006"[10], banks and financial institutions were made to focus on cheques and online banking fraud which further limited computer crimes related to financial institutions.

It's a clear fact that computer crimes will not disappear completely, however it could be seen that United Kingdom has taken some steps to limit the computer crimes to a greater level. Although circumstances are as such, it is a felt need that relevant provisions must be always updated since computer crimes keeps developing with the advancement of technology.

Computer crimes and related law in Sri Lanka

Computer Crimes is considered as a novel aspect in the criminal activities of Sri Lanka. 'Ilya Ehrenberg'[11] statement is dedicated to make Sri Lanka the wonder of Asia today has to focus on the aspect of Computer Crimes which has become a great threat to the whole world. With the development of Information Technology and Computer Science in Sri Lanka people tend to focus on Computer Crimes as a way acquiring wealth. Fact pointed out in Ilya statement is once again highlighted because most of the persons affected by computer crimes are youth around the world.

Computer Crimes Act no 24 0f 2007[12] which defines a computer as an electronic or similar device having information processing capabilities was designed with the objective of providing identification of computer crime and to provide the procedure for the investigation and prevention of such crimes and to provide for matters connected therewith and incidental thereto.

Section 2(1)[13] defines that act shall apply where;

> (a) A person commits an offence under this Act while being present in Sri Lanka or outside Sri Lanka;
>
> (b) The computer, computer system or information affected or which was to be affected, by the act which constitutes an offence under this Act, was at the material time in Sri Lanka or outside Sri Lanka.

[9] *Police and Justice Act 2006,* united kingdom, <http://www.legislation.gov.uk/ukpga/2006/48/contents> accessed 11 th April 2020

[10] *Fraud Act 2006,* united kingdom,<http://www.legislation.gov.uk/ukpga/2006/35/contents> accessed 11 th April 2020

[11] 'ERENBURG, Ilia, 1891 -1967' <http://connection.ebscohost.com/tag/FRENBURG%2C+Ilia52C+1891-1967> accessed on 12 th April 2020

[12] *COMPUTER CRIME ACT,NO 24 of 2007,* http://www.slcert.govt.lk/Downloads/Acts/computer_crimes_Act_No_24_of_2007(E).pdf accessed on 12 th April 2020

[13] ibid

ISSN 1800-055X Vol. Iv

(c) The facility or service, including any computer storage, or data or information processing service, used in the commission of an offence under this Act was at the material time situated in Sri Lanka or outside Sri Lanka; or

(d) The loss or damage is caused within or outside Sri Lanka by the commission of an offence under this Act, to the State or to a person resident in Sri Lanka or outside Sri Lanka

It is also important to focus on the offences that have been highlighted under section 3[14] of the act which states that any person who intentionally does any act, in order to secure for himself or for any other person, access to,

(a) any computer; or

(b) any information held in any computer, knowing or having reason to believe that he has no lawful authority to secure such access, shall be guilty of an offence and shall on conviction be liable to a fine not exceeding one hundred thousand rupees, or to imprisonment of either description for a term which may extend to five years, or both such fine and imprisonment.

Section 4[15] is an expansion to section 3(b) which states that any information held in any computer, knowing or having reason to believe that he has no lawful authority to secure such access and with the intention of committing an offence under this Act or any other law for the time being in force. Section 4 therefore focuses on applicability of the act or any other law prevalent in the country.

The Act does not expect criminal intention to use the computer to commit an offence. Section 17(1)[16]of United Kingdom Computer Misuse Act defines about access which states that; A person secures access to any program or data held in a computer if by causing a computer to perform any function he,

(a) Alters or erases the program or data;

(b) Copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) Uses it; or

(d) Has it output from the computer in which it is held (whether by having it displayed or in any other manner); and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

However, Sri Lankan Computer Crimes Act does not have an interpretation for the term access as in United Kingdom act.
According to an article on Sunday Leader newspaper by Kashman Indrajith Keerthisinghe[17] the number of cybercrimes complaints have shown an increase according to reports of Computer Emergency Response Team (SLCERT). The reports further reveal that most of the complaints in Sri Lanka relate to hacking passwords, stealing of information,

[14] ibid
[15]ibid
[16]*computer misuse Act 1990*<http://www.legislation.gov.uk/ukpga/1990/18/section/17> accessed on 12 th April 2020.
[17]Kashmanindrajithkeerthisinghe,(2020) *The Sunday leader,* 15 Jan .<http://www.Thesundayleader.lk/>

ISSN 1800-055X Vol. Iv

demanding ransoms in addition to Facebook and credit card related crimes.

It is also important to focus on the Intellectual Property act no 36 of 2003 when computer crime related acts are concerned. According to section 178(1)[18], any person who willfully infringes any of the rights protected under Part II of this Act shall be guilty of an offence.

- Any person knowing or having reason to believe that copies have been made in infringement of the rights protected under Part II of the Act, sells, displays for sale, or has in his possession for sale or rental or for any other purpose of trade any such copies, shall be guilty of an offence…

- Any person knowingly or having reasons to believe that he is in possession or has access to a computer program infringing the rights of another person, and willfully makes use of such program for commercial gain, shall be guilty of an offence.

Moreover Sri Lanka Telecommunications Act section 53[19] which relates to telecommunication transmission holds that Every person who willfully seeks to intercept and improperly acquaint himself with the contents of any telecommunication transmission not intended for general reception shall be guilty of an offence, and shall be liable on conviction to a fine not exceeding ten thousand rupees or to imprisonment of either description for a term not exceeding six months or to both such fine and such imprisonment.

Investigation procedure for these criminal activities is also of wide importance. Section 15[20]holds that except as otherwise provided by this Act, all offences under this Act shall be investigated, tried or otherwise dealt with in accordance with the provisions of the Code of Criminal Procedure Act, No. 15 of 1979. And moreover section 16[21] holds that every offence under this Act shall be a cognizable offence within the meaning of, and for the purpose of, the Code of Criminal Procedure Act, No. 15 of 1979 where by a person may also be arrested without a warrant.

Law relating to computer crimes in Sri Lanka must be amended and updated considering the changing technology and new trends of computer crimes like in United Kingdom. However United Kingdom is considered as a country in which a higher number of computer crimes are reported. Because of this reason, authorities in United Kingdom implement laws and appoint bodies to govern such crimes whenever it's required. In Sri Lanka computer crimes are considered as a novel concept but it is found that rate at which computer crimes being recorded show a rapid growth therefore implementing such an action would result in reduction of computer crimes in Sri Lanka to a greater extent.

[18] *Intellectual property act no 36 of 2003, <https://www.lawnet.gov.lk/1946/12/31/intellectual-property-3> Accessed on 12 th April 2020*

[19] Sri lanka Telecommunication Act(No.25 of 1991), Sri lanka<http://www.commonlli.org/lk/legis/num_act/slta25o1991337/> accessed on 12th 2020

[20] *computer crimes Act No 24* of 2007, srilanka<http://www.slcert.gov.lk/Downloads/Acts/computer_crimes_Act_No_24_of_2007(E).pdf > accessed on 12th April 2020.

[21] Ibid

ISSN 1800-055X Vol. Iv

It would be better if limitations are imposed by producers and owners of software and applications so that copies of such products will not be sold illegally by third parties. Although precautionary steps are taken, it is an undoubtable fact that copies of software are made, therefore owners can design special applications to detect illegal software when installed to a computer.

It is paramount important that users of internet must be given knowledge of criminal acts done though computer and internet. In countries like Sri Lanka computer crime is a novel concept and users of internet at most of the time are not aware of the crimes that take place through internet. Therefore, relevant authorities must take actions to provide knowledge to persons who do not have sufficient knowledge about such crimes and must pay special attention to persons who do not have sufficient knowledge

Most of the time persons who are engaged in computer crimes engage in such acts due to the availability of high protection that is available to conduct such malpractices.

The main reason for this is because when computer crimes are being conducted, personal identity is not revealed. In such cases, it would be better if data are stored to computers in a way that personal identity is revealed.

In Sri Lanka a national initiative is urgently required to tackle the issue of computer crimes. If such a national initiative set of laws are available, then most of the crimes can be solved at national level leading to no involvement in international law. Further it needs to be applied across Sri Lanka and needs to be a part of transnational effort whereby such set of laws have the acceptability of the world. When such laws are designed it must made sure that those confine with international standards and have the capability of governing computer crimes that keeping growing with the advancement of technology.

The government must also take actions to conduct seminars and programs that could educate general public about trending computer crimes and they should informed about the harmful effects that take place due to computer crimes.

Government must take actions to impose severe punishments for those who engage in computer crimes. It is quite acceptable that when punishments are made more severe people would not tend to engage in certain types of crimes. So this procedure could be applied to reduce computer crimes that keep growing in Sri Lanka. Further such an act would reduce the crimes that could take place in future as well.

The level of unemployment of the country too can result in the growth of computer crimes. Some persons those who have good knowledge regarding computers and internet engage in computer crimes and such malpractices for the sole purpose of enjoying monetary benefits. Therefore, being a developing country, Sri Lanka too must focus on answering the issue of unemployment and providing employment opportunities for persons considering their level of knowledge and intelligence. Such an act could bring down the computer crime rate that keeps growing along with the advancement of technology.

Therefore having analyzed above circumstances it could be identified that current law in Sri Lanka regarding computer crimes has to be amended and updated. This is because computer Crimes is a type of a crime that keeps developing with the advancement of technology and

ISSN 1800-055X Vol. Iv

really needs to be compatible with international law regarding computer crimes. However, in United Kingdom unlike in Sri Lanka, computer crimes are being reported at a high rate and authorities in United Kingdom have taken due steps so far by amending and updating relevant law to overcome such issues. Available provisions in United Kingdom could be used as a supporting factor to amend law in Sri Lanka in a way that loopholes or gaps that exist in Sri Lankan legal system would be filled.

ISSN 1800-055X Vol. Iv