|  |
| --- |
| IS-2220  Essentials of law-L2S2 |
| **Computer Crimes Law** |
|  |

|  |
| --- |
| **185049V M.F.F. Nifla**  **184006F M.F.F. Ahmed**  **184112C T.P. Nusra**  **Date of Submission: 2021/03/10** |

**Introduction**

In this 21st century, Information and Communication Technology (ICT) plays a vital role in our lives. With the emergence of ICT, the internet and electronic commerce have become important in day-to-day life and it created the global village. Thus, the need for development in the ICT sector is compulsory; on the other hand, the rise of crimes that are connected to computers—which have been recognized as “computer crimes” or “cybercrimes‟—also increasing day by day. Computer-related crimes in which computers used as tools for criminal activities such as theft, fraud, etc.; hacking offenses and introduce viruses, worms, etc. which effects integrity, availability, and confidentiality of a network or computer system; and content related computer crimes where computers and internet are used to distribute illegal data such as child pornography through the internet are mainly three types of computer crimes.

Sri Lanka is a developing country that is not so expertized in the ICT industry when comparing with the European and other developed countries. But when comparing with the situation of Sri Lanka in the past two decades, there is no doubt in saying that it is much more developed. The criminal justice system of Sri Lanka assists the ICT industry of our country to develop it. It provides securities to prevent cybercrimes and other offenses which are being done by

computers.

**Types of Computer Related Crimes.**

The use of information technology for criminal reasons or improper access to a computer system with the intent to destroy, erase, or change the data stored on the server is referred to as computer crimes. Identity stealing, software misuse, and electronic fraud are all considered computer crimes.

Old offenses were carried out using computers as a tool: for example, unauthorized photos were stored on a hard disk instead of being printed, and abuse was carried out using cell phones. ‘Phishing' is another example.

New technologies have enabled new forms of crime. Denial of service (DOS) attacks, for example, block network services from being made accessible to intended users by loading web servers with more data than they can handle.

Now Let’s see a brief explanation about different types of computer crimes.

1. Hacking

Hacking is the act of defeating a computer system's protection capability to gain unauthorized access to the information contained on the computer system. Another very serious cybercrime is the hacking of IP addresses to trade under a fake name and remain anonymous when committing illegal acts.

1. Phishing

Phishing is an act of trying to obtain personal information, such as usernames, passwords, and credit card numbers, by disguising it as a reliable source. Phishing is done through emails or by tricking users into entering personal details on fake websites.

1. Computer Viruses.

There are, in reality, computer programs that are capable of replicating it and damaging the computer systems present in the network. These viruses operate without the awareness of users and travel from one machine to another via the network, the Internet, or portable devices such as CDs and USB drives. A computer virus writing is an illegal offense that is punishable by law.

1. Identity theft.

This is one of the most serious frauds in today's world. It means taking money and making a profit by using someone else's name. This often requires the use of someone else's credit card information to buy goods and services. It has been shown that blackmail and extremism were also involved in identity theft.

1. Cyberstalking

This is where someone uses the Internet to stalk someone in the same way they will in the real world. Here, the stalker sends emails, shares fake facts, or threatens to use the Internet. Cyberstalks also threaten users via chat rooms, internet forums, and social networking platforms to harvest user information and annoy users based on the information they collect.

**Computer Crime Laws in Sri Lanka**

Penal Code, Criminal Procedure Code, and Evidence Ordinanceare some main legislation that deals the crimes in Sri Lanka. Penalties and sanctions are given by the courts to the convicted persons as punishments. Basically, the crimes which fall under these laws are done physically and they cause death, injury, or loss to the victim. Whereas, in computer crimes, there are no such physical injuries or violence taking place, but they are similar and serious as the traditional crimes.

For instance, if someone has stolen or damaged the data which was saved in another one‟ computer, then that is similar to theft. But it is impossible to fulfill the requirements which have been required by laws to prove the theft; because the thing which has been stolen has to be tangible. It is the main criteria that establish the crime „theft‟. But data or documents saved on a computer are intangible. Thus, there was a need of enacting laws to deal with computer crimes in the ICT industry.

**COMPUTER CRIME ACT**

Computer Crime Act is an Act to identify and arrange for prosecution and prevention of computer crimes and to deal with matters related to them and incidental to them. Computer Crimes Act has been recognized a number of computer crimes and it guarantees protection from such crimes. It plays an important role in the criminal justice system in the ICT industry of Sri Lanka.

Part 1 of this Act specifies the computer crimes and the sanctions for that; part 2 explains the process of investigations. Major computer crimes are mentioned in sections 3 to 10.

Computer Crimes Act of Sri Lanka has been enacted section 3 which says,

“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 5 explains the offence of causing a computer to perform a function without lawful authority. This sort of offences taking place due to the distribution of a program called „logic bomb‟ and it would destroy the programs of the computer automatically if there is no proper firewall or guard.

Section 6 of the Computer Crimes Act states,

(1) Any person who intentionally causes a computer to perform any function, knowing or having reason to believe that such function will result in danger or imminent danger to—

(*a*) national security;

(*b*) the national economy; or

(*c*) public order,

shall be guilty of an offence and shall on conviction be punishable with imprisonment of either description for a term not exceeding five years.

For instance, uploading flips or opinion pieces through websites that threaten national security (known as cyber-terrorism), or logging into the banned websites, or insulting and attacking religious leaders; articles that damage the Sri Lankan economy are considered crimes under this section.

Section 7: illegal to upload or download anything without the permission of the website owner

Likewise, from section 3 to 10 the Computer Crimes Act specifies some major crimes which have been done through computers.

 Other than the Computer Crimes Act, the Payment Devices Frauds Act, Electronic Transactions Act, Intellectual Property Act, Prevention of Money Laundering Act, Financial Transactions Reporting Act etc. also passed by the legislators of Sri Lanka to prevent crimes and to develop ICT industry of the country.

**Challenges in implementing laws against Computer Crimes**

Hence, a plenty of Acts and Ordinances and institutional mechanisms have been created by the parliament of Sri Lanka to develop the ICT industry and to prevent computer related crimes. However, there are also drawbacks which could be identified in ICT industry in the Sri Lankan context. Those shortcomings have to be addressed in ICT industry to move on with the emerging trends of the world.

In Sri Lankan context, the ICT industry is not very developed when comparing with the western and other developed countries. Even though the laws are guaranteed the security from the cybercrimes, there are no proper advanced technologies have been adopted. It is an undeniable fact that Sri Lanka is still lacking advanced technologies and technicians in ICT industry to carry on the criminal investigation process.

Even though the Computer Crimes Act is a newly adopted to address the computer crimes, still there are shortcomings identified on that and there are practical impossibilities in applying those laws. When we take section 7 of this Act, it is illegal to upload or download anything without the permission of the website owner. But these kinds of offences are very common in our country. There is no any security measures have been taken to protect such intellectual properties.

And also it could be said that people are ignorant about computer related offences and they do not know the seriousness of such crimes. And some people do not know what cybercrimes are. Therefore, there are many things which have to be shaped by the criminal justice system of Sri Lanka to develop the ICT industry of the country and prevent from computer related crimes.

**Conclusion**

As mention above there are many drawbacks and shortcomings in computer crime laws in Sri Lanka. According to that, adopting new technologies on investigation process in ICT industry; adopting security measures to secure the intellectual property rights; introducing new types of defenses on cybercrimes which would be more suitable; Adopting foreign countries‟ methods in investigation processes which are related to ICT; conducting awareness programs and workshops on cybercrimes; making ICT as a compulsory subject in school levels; and giving effect to the computer crime laws through judicial decisions can be recommended.

Thus, are the conclusion, it can be recognized that in Sri Lankan context, even though the laws are there to develop the ICT sector, they have to be given a push up by the criminal justice system of the country.