Computer Crimes Law

IS 2220 – Assignment 2

❖ Group Members –

- 184136D – Rajapaksha R.A.P.D
- 184101R – Marapana T.N
- 184060M – Jayaratha H.M.D.T
- 184132L – W.A.R.Prasadini
- 185035B – Jayathilaka M.D.S.S

- Date of submission – 14/03/2021

Introduction

(Computer crime and act)

The organized climate has set out open doors for Governments, organizations and clients. Thus for these improvement quantifies, the ICT education alone in the nation has expanded. In any case, this expanded use has brought about difficulties showed as misuses and abuses. Sri Lanka reacted to challenge by sanctioning the Computer Crimes Bill. This Bill, which was affirmed by the Speaker of Parliament on 9" July 2007, as Computer Crimes Act No. 24 of 2007.

In light of this bill during the beginning phases of the Drafting cycle the arrangements contained in the Penal Code of Ceylon were analyzed to decide if the Penal Code could be altered to adjust to manage Computer Crime related offenses.

Notwithstanding, it was felt that meanings of offenses, for example, Cheating and Criminal Misappropriation in the Penal Code of Ceylon restricted mirror the conditions that won in the earlier century. It was tracked down that those definitions were figured with the understanding that a recognizable human wrongdoer and casualty are in presence and imagined the commission of a demonstration in a predetermined way by the guilty party against the person in question.

There are two terms as "Computer Crime" and "Computer Crime"

Computer Crime is a conventional term used to distinguish all crimes or fakes that are associated with or identified with computers and data innovation.

"Cyber Crime" will in general be focused towards crime coming about because of the utilization of the web.

Cyber Crime computer crime is the thing which characterized in the Act and lawmakers.

Under this document, we going to discuss about,

Act would apply where in crimes law , In terms of substantive offences the Sri Lankan Computer Crime Act covers a broad range of offences, which could broadly fall into the following two categories of offences. Some of the key substantive offences under the computer crimes act are..

Computer Crime Act would apply where

The computer crime Act of Sri Lanka is certified in 2007 as Act No 24 of 2007. It is very important for all the people in Sri Lanka to know where would applicable this Act. And also what is in this act. According to the Computer Crime Act of Sri Lanka, it is considered as a crime like accessing other people's computers without permission and change their details, data destruction also consider a crime.

The following are the areas where this Computer Crime Act applies.

- If a person commits an offence under this act, he is guilty of that offence whether he is in Sri Lanka or outside of Sri Lanka.

- Under this law of crime act The computer, computer system or information that is affected for offence are located in Sri Lanka or outside of Sri Lanka wherever it is applicable under this act.

- The facility or service including computer storage or information processing service used for an offence were situated in Sri Lanka those are applicable under this act.

- where the loss or damage is cased wherever in Sri Lanka or outside Sri Lanka by the commission of an offence under the act, it is an applicable person who resident in Sri Lanka or outside Sri Lanka.

As mention above the Sri Lankan computer crime Act covers a board range of offence. The computer-related crimes and hacking offence are broadly covered. It is very valuable for all people

to be aware of this computer crime law because a lot of people get into computer crime offence without having any awareness.

Components of computer crimes

In terms of substantive offences, the Sri Lankan Computer Crimes Act covers a wide range of offences that can broadly be divided into three categories.

(01)Computer-related crimes

(02)Hacking offences

(03)Content-related Cyber Crime

Computer-related crimes

Where computers are used as a tool for criminal activity such as fraud, theft, and so on.

Fraud is a type of property crime that occurs when someone uses deception or trickery to gain an unfair advantage. As a result, the deception may be carried out with the consent of the person or organization deceived.

When someone commits fraud, they frequently conceal their actions, so the crime often goes unnoticed for a long time. It's possible that the fraudster did not even come into direct contact with the victim.

Computer fraud is defined as illegally gaining control of a computer or stealing information without the knowledge of others. It can take many forms, including fraud committed by a company employee who uses a computer to steal funds or information from the company, as well as a deception to gain access to individual resources

The type and method used to commit computer fraud differ from person to person, depending on the need for it.

Computer fraud can be classified in a variety of ways depending on the type of fraud committed, but the most common types are listed below.

- Internet auction/Bid sales fraud
- Retail sales
- Investment schemes
- Credit card fraud
- Information hacking
- Email hoax

Theft occurs when someone takes or steals something that belongs to someone else without their permission. To be proven guilty of theft, the accused must first intend to commit the crime and then successfully deprive the victim of their property.

Hacking offences

Hacking offences have an impact on a computer system's or network's integrity (data is accurate and trustworthy and has not been modified), availability (data, services, and systems are accessible on demand) and confidentiality (networks, systems, and data are protected and only authorized users can access them).

The term "hacker" has several meanings, and can refer to someone who investigates programmable systems, is obsessive about programming, can program quickly, or is an expert in a specific program. It's difficult to match the common understanding of what constitutes computer hacking with anti-hacking laws because of these meaning overlays.

Hacking isn't always a crime because "ethical hacking" occurs when a hacker is allowed to exploit security networks under permission. To put it another way, it's when a hacker has the necessary permission or authorization. Hacking, on the other hand, crosses the criminal line when a hacker gains access to someone's computer system without their permission or authority.

For example, an individual can be charged with a crime if they breach a company's firewall to gain access to private servers and cloud storage systems, or if they use phishing to install malware on desktop computers with the intent to monitor communications and activities without consent or any lawful authorization.

- Worm-Standalone malicious software that does not require a host, copies itself from one computer to another and does not usually target files on a single computer.
- Virus-A computer virus is a malicious program or code that is written to change the way a computer works and is intended to spread from one computer to another. In order to execute its code, a virus inserts or attaches itself to a legitimate program or document that supports macros. It requires user activity to spread.
- Trojan horse-Malware that imitates legitimate software in order to trick the user into downloading the program, then infects the user's system and allows the malware to steal, spy or harm.
- Spyware-Malware designed to surreptitiously monitor infected systems, and collect and relay information back to the creator and/or user of the spyware.

Content related Cyber Crime

Other types of cybercrime are content-related and involve the production, procurement, distribution, offering, and possession of online content that is considered illegal under national laws.

Where computers together with Internet resources are used to distribute illegal data. Eg: Internet based pornography, criminal copyright infringement.

The Berne Convention for the Protection of Literary and Artistic Works of 1886, the World Intellectual Property Organization (WIPO) Agreement on Trade-Related Aspects of Intellectual Property Rights of 1994, and the WIPO Copyright Treaty of 1996 are all international treaties relating to copyright protection. In the case of intellectual property, there are also regional laws. Digital piracy is a well-known example of infringement of copyright protection.

Example:-unauthorized copying, duplication, or distribution of a movie protected by copyright law.

Intellectual property encompasses not only copyrights but also trademarks (brand names, symbols, or logos) patents, and trade secrets.

In recent years, the most contentious issue arising from the use of the Internet has been pornography. The government, law enforcement bodies such as the police, prosecutors, and judges, as well as the media in general, have expressed fear and "moral panic" as a result of its availability on the Internet.

There are many laws in this regard in our country as well as in other countries of the world.The Government of Sri Lanka has recently implemented a number of measures to curb pornography in the country, including censoring pornographic websites and prosecuting Sri Lankans who have appeared on these types of websites.

Key provisions of Computer Crimes Act

The following are some of the major offenses committed under the Computer Crimes Act,

- Section 3 of the Act denotes that a criminal has no legal right to gain access to a computer or to secure information contained on any computer. Knowing that the offender has no legal authority to obtain such access.
- Section 4 of Act criminalizes unauthorized access with intent to commit another offense under the Computer Crimes Act or any other law.
- Section 5 causes a person to perform a function on a computer that causes unauthorized alteration and damage to a computer, computer system, or computer program.
- Section 6 deals with economic and national security offenses committed by a computer.
- Section 7 makes it an offense to purchase, receive, upload or download information illegally obtained from a computer or storage medium.
- Section 8 unlawfully intercepts subscriber information or traffic data or any communication within a computer.
- Under Section 9 of the Computer Crimes Act, activities such as the manufacture, sale, import and export and distribution of computer related things or computer passwords or access codes may be a criminal offense.
- Section 10 denotes with unauthorized disclosure of information that may be accessible to a Service.

When we consider about close review of a wide range of offenses under the above Sri Lanka Computer Crimes Act demonstrates the level of compliance with the Council of Europe Convention on Cybercrime. With respect to content of the cybercrime, it has been enhanced the scope Intellectual Property Act 36 of 2003. In addition to introduced penal code in 2006. This offence was introduced prior to the Computer crimes Act. Further, in Sri Lanka introduced the Payment Devices Fraud Act No.30 of 2006 for deal specifically with the possession and use of unauthorized payment instruments.

Investigation and enforcement

Law enforcement investigations close cases and can prevent new crimes from occurring. Training in research-based investigative procedures and access to tools and resources can help law enforcement officers carry out successful investigations.

Any criminal examination meddles with the privileges of others, regardless of whether the individual is the subject of an examination or a connected outsider. In a vote-based society any such obstruction should be reasonable and proportionate to the necessities of society looked to be secured. Notwithstanding, the development of organization-based wrongdoing has brought troublesome issues up in regard of the fitting harmony between the necessities of those researching and arraigning such wrongdoing, and the privileges of clients of such organizations.

Moreover, there are the rights and interests of the organization suppliers, the middle people that form and, or, work the organizations and administrations, through which information is imparted.

These difficulties expect gatherings to a requirement interaction, specifically specialists, examiners and judges to work in a planned way. This "essential co-appointment"

5 New Sections 286B and 286C presented through Penal Code (Amendment) Act No. 16 of 2006

Is likewise trying for Governments as a result of the absence of ability to regularly manage Cyber Crime. As such Governments have been constrained to depend on mastery outside governments, like Academia and Business.

This is the involvement with Sri Lanka too. The Sri Lankan Computer Crimes Act reacted to these requirement challenges by accommodating an "autonomous" gathering of specialists to help Law implementation organizations in the examination of Cyber Crime6.

These assigned specialists are completely enabled and given security under the legislation7. The presentation of the idea of a “specialist” in the Act is to guarantee that getting to of a PC is done simply by talented assets, equipped for playing out a proficient location while simultaneously guaranteeing that the PC equipment and programming isn't harmed.

Shields have likewise been worked in to ensure the organizations and Computer frameworks that are being investigated8. This to give the "comfort" measures for organizations and people to Report Cyber Crime.

Conclusion

Information assumes an essential part in the commission of numerous cybercrimes and weaknesses to cybercrime. Despite the fact that information gives clients of it with incalculable freedoms, these advantages can be misused by some for criminal purposes. In particular, information assortment, stockpiling, investigation, and sharing both empowers numerous cybercrimes and the tremendous assortment, stockpiling, use, and circulation of information without clients' educated assent and decision and vital legitimate and security assurances.

Likewise, information total, investigation, and move happen at scales that legislatures and associations are not ready for, making a large number of network protection chances. Protection, information insurance, and security of frameworks, organizations, and information are associated. Taking into account that, to ensure against cybercrime, safety efforts are required that are intended to secure information and client's protection.

References:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3690552

https://www.oas.org/juridico/spanish/cyber/cyb3_cc_law.pdf

https://www.slideshare.net/VishniGanepola/computer-crime-and-the-adequacy-of-the-current-legal-framework-in-sri-lanka

https://rm.coe.int/16802f264b