Has Sri Lanka worked out effective ways of fighting computer crime? – An analysis in respect of investigations under the Computer Crime Act of 2007

Selvaras Janaha[1]

Department of Legal Studies, Faculty of Humanities and Social Studies, The Open University of Sri Lanka, Nawala, Nugegoda, Sri Lanka

sjsjanah@gmail.com

Abstract— *"Adapt yourself to the changes in the world." This is the natural rule of world. In the light of this rule, countries of the world have accepted the revolution of technology. Information technology has entered people's lives in the past few decades. Sri Lanka is not an exception to these changes; we can witness main areas of the Information Technology in Sri Lanka such as e-commerce, intellectual property, computer evidence and forensic issues.*

Trends are developing to shift the nature of crimes from traditional to hi-tech. Therefore, the computer has become a tool for committing crime. This paper examines to what extent the steps taken so far have been effective in fighting computer crimes in Sri Lanka. The research questions are: Has Sri Lanka worked out effective ways of fighting computer crimes? To what extent are legal provisions of investigations helpful in protecting citizens from computer crimes?

This paper focuses on the Computer crimes in Sri Lanka and its implementation. Therefore this paper mainly discusses the investigations under the Computer Crimes Act No 24 of 2007 and its components and loopholes. This paper adopts certain analytical methods in approaching this issue.

According to the Computer Crimes Act of Sri Lanka, "Computer Crime" is used to cover all crimes and frauds that are connected with or related to computer and information technology. In addition, Sections 15 to 24 in part II of this act contain the law on investigations.

Even though we have provisions on computer crimes and investigations, there are practical problems with the existing law. Further, different countries have adopted different policies on cybercrimes and cybercrime investigations which have been left out in our Act.

At the moment we may not have countless victims affected by computer crime except traditional offences, it is our duty to take precautionary measures regarding this issue and take serious concern on investigations of computer crimes and cybercrimes.

Keywords— **Computer crime, Computer Crimes Act of Sri Lanka, Investigations**

I. INTRODUCTION

This paper attempts to describe the Sri Lankan Computer Crimes Act 2007 and discuss significant features of successful computer crimes investigation under the Act. The legislative enactment of Computer Crimes Act of 2007 is a step in the right direction for a developing country like Sri Lanka as it attempts to walk forward as a knowledge hub. However having laws alone will not be sufficient to carry out trials on computer crimes. Therefore the most important element of a computer crime – Investigation- is discussed in this paper. Furthermore this paper is going to study the methods followed by developed countries in regard to this to carry out our path.

This research aims to provide a clear picture of the nature of the computer crime and investigation under the Act and also whether the existing investigation system is sufficient to handle cases in future.

A) Methodology

Since the less number of cases available in this field is less, this paper adopts the analytical methods in approaching the topic.

B) Traditional Crimes Vs Computer Crimes

The term "Crime" can be defined as "a positive or negative act in violation of a Penal law". A crime is also defined as an act done in violation of the duties an individual owes to the community. Breach of such duty is provided with a punishment in Law. While in certain jurisdictions the word "crime" is used to define a prohibited act or omission under a penal law, Sri Lankan Penal Code has used the term "Offence" to define such acts and omissions. - Sec 38(1) of the Penal Code.

Our law recognizes the latin maxim "actus non facit reum nisi mens sit rea" which means 'nothing is an offence which is done without a criminal intent'. Accordingly an offence has two main elements; the physical act or the omission (actus reus), and the mental element (mens rea).

The term "Crime" has been interpreted in many ways. According to Black's Law Dictionary "a crime" is defined as "an act done in violation of those duties, which an individual owes to the community and breach of which the law has provided that the offender shall make satisfaction to the public". – Blacks' Law Dictionary- 6th Edition page 370

Computers have proven to be valuable assets of each and every human being and almost every sector of computers internationally and nationally leads this society to e-commerce, e- communication, e-research and computer based record keeping. While the number of computer usages increase the nature of offence and the number of offences have started demanding attention of legislators.

The broader definition of computer crime is, a crime in which the perpetrator uses special knowledge of computers (Furnell, S.(2002) Cybercrime: Vandalizing the Information Society. London: Pearson Education Ltd)

Computer crime means a criminal activity where a computer or network is the source for the crime. Broadly it can be defined as criminal activity involving an information technology infrastructure, including illegal access, illegal interception, data interference, and systems interference, misuse of devices, forgery, and electronic fraud. The crime can target computer network or device directly or facilitated by computer networks or devices.

C) Overview of the Computer Crimes Act 2007

In Sri Lanka the general substantive law which is applicable for criminal activities is Penal Code of 1885. Penal Code deals with the offences against persons and property. Sri Lankan penal code does not define the term property. Still movable property is defined to include 'Corporal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth'. (Section 20 of the Penal Code) In case law, Nagaiya V Jayasekera,(1927) 28 NLR 467 it was accepted that the definition given to property was not exclusive to deal with contemporary information and communication technology related offences. Even early attempts to include intangible property within the existing definition were rejected by the Supreme Court, which it held that electricity was not "property" within the meaning of the penal code.

Hence the definition given to "property" and other definitions for wrongful acts in the penal code are inadequate to deal with the criminal activities, such as contemporary information and communication technology. Since it was decided to do the needful the Committee on Law and Computers of the Council for Information Technology of Sri Lanka proposed the current Computer Crimes Act of 2007.

Generally a Computer Crime includes three components. They are, Computer related crimes, hacking offences and content related cybercrimes. Computer related crime means where computers are used as a tool for criminal activity such as theft, fraud etc; hacking offences mean those affect integrity, availability and confidentiality of a computer system or network (also includes the introduction of Viruses, worms etc); and content related cybercrime means – where Computers together with internet resources are used to distribute illegal data. Eg. Internet based pornography, Criminal copyright infringement. But our Act only deals with the first two components.

It is relevant to differentiate Computer crimes from Cybercrimes at this point. Computer crimes are non-traditional crimes that have arisen directly from the advent of the age of personal computing for managing information and communication. Cybercrimes is a criminal activity committed through the use of electronic communications media.

The scope of the computer crimes act is wide enough to include the offenders globally. For example if a person commits an offence while being in Sri Lanka is cause loss or damage to the state or is a person who is residing in Sri Lanka or outside with the use of computer, computer systems, information facility or service, computer storage or data information processing service, he could be dealt under this Act.

D) Offences under the Computer Crimes Act

Identified offences under the computer crimes Act are, Offences relating to Unauthorized Access (sec 3 of Act) , Ulterior Intent Offence (Sec 4 of Act), Unauthorized Modification of Material (Sec 5 of Act), Offences against National Security, Public Security and National Economy (Sec 6), Involvement with data illegally obtained (Sec 7 of Act), Illegal Interception of Data (Sec 8 of the Act), Using of Illegal Devices (Sec 9 of the Act), Unauthorized Disclosure of Information enabling Access to a Service (Sec 10 of the Act), Attempts to Commit Offences and Abetment and Conspiracy (Sec 11 of the Act).

Since this paper focuses on the Offences Relating to Unauthorized Access, it has omitted the explanation of rest of the offences under the Act.

E) Investigation under Computer Crimes Act 2007

The new Act on Computer Crimes introduces a new regime for the investigation of offences against computers. The value of the legislation is subject to the efficiency and effectiveness of the investigation system.

Sections 15 to 24 in part II of this Act contain the law on Investigation. This part describes the process of investigation and the salient features of investigation under the Act. Section 15 states 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. (Sections 109- 125 of the Code of Criminal Procedure Act No 15 of 1979 are applicable)

Section 16 of Computer Crimes Act defines 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. By this definition it is visible that any person committing any offence under this Act maybe arrested without a warrant.

The success of computer crimes investigation depends on the effectiveness of the investigative team. According to Section 17 (1) of this act the minister who is in charge of Science and Technology is the one who appoints the expert team to assist the police officer who handles the investigation. By this section following person mean the term "expert", any member of the staff of any university who possesses the prescribed qualification and nominated by the Vice-Chancellor of the relevant University or any public institution. (According to Sec 17 (2) (c) of the Act, University shall mean any University established under the Universities Act, No 16 of 1978.)

Computer Crimes Act empowers an expert to, enter into any premises along with a police officer not below the rank of a sub-inspector, and access any information system, computer or computer system or any programme, data or information held in such computer to perform any function or to do any such other thing, require any person to disclose any traffic data, orally examine any person, and to do such other things as may be reasonably required, for the purpose of this Act. (Section 17(4) (a) (b) (c) (d) and (e)).

In addition to that, the Act also allows that an expert shall be paid such remuneration as may be determined by the minister in consultation with the Minister in charge of the subject of Finance. (Section 17(5)

Section 18 (2) of the Act provides authority to an expert or a police officer to conduct warrantless searches ,if the investigation needs to be conducted urgently since there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible and to maintain confidentiality regarding the investigation. Other than this for the purposes of obtaining any information including subscriber information and traffic data in the possession of any service provider, intercepting any wire or electronic communication including subscriber information and traffic data, at any stage of such communication, the expert or the police officer should get a search warrant by making an application to the Magistrate Court. (The provisions of the Criminal Procedure Code Act No 15 of 1979 would apply in terms of such warrants)

It is important to mention here what is meant by the term "Service provider". It is a public or private entity which provides the ability for its customers to communicate by means of a computer system or any other entity that processes or stores computer data or information on behalf of that entity or its customer. (Interpreted in Section 38 of Computer Crimes Act)

It is the responsibility of an expert or a police officer to protect the data needs to be protected by taking necessary steps. Therefore the Act allows that, If there is a risk of that such information being lost, destroyed, modified or rendered inaccessible and in such an event they may by written notice require the person in control of such computer or computer system to ensure that the information be preserved for such period not exceeding 7 days as may be specified in such notice. (Section 19 (1) of this Act) Also if such protection is to be continued, the expert or the police officer can make application to the Magistrate to extend the period of protection for a period not exceeding 90 days. (Section 19(2) of the Act)

The way the Act empowers an expert and a police officer; it imposes a set of duties to every police officer and every expert who conducts an investigational search. They must make every endeavor to ensure that the ordinary course of legitimate business for which any computer may be used is not hampered by such search, inspection or investigation and shall not seize any computer, computer system or part thereof, if such seizure will prejudice the conduct of the ordinary course of business for which the computer is used. (Section 20 of the Act) The exception to the above mentioned duty is that, a police officer or an expert may seize or take in to his custody any such computer only if it is not possible to conduct the inspection on the premises where such computer, computer system or part thereof is located or seizure of such computer, computer system or part thereof is essential to prevent the commission of the offence or the continuance of the offence or to obtain custody of any information which would otherwise be lost, destroyed ,modified or rendered inaccessible. (Section 20 of the Act)

Section 21 of the Act deals with arrest, search and seizure of information. Although the relevant officers mentioned by this act can conduct warrantless search, they are required to produce such suspect immediately and without delay before a Magistrate's Court (Section 21(1)) and this section strictly mentions that every police officer who commences an investigation under this act is expected to have a certificate issued by the Inspector General of Police in writing confirming that such police officer possesses adequate knowledge and skill in the field of Information Communication Technology and thereby possessed of the required expertise to be involved in such a function. (Section 21(2))

In terms of duty of Police officers upon seizure, this act provides an obligation on every police officer who seizes or takes into custody a computer or any other item or data, to immediately issue a complete list of such seizure. This list must be issued to the owner or the person in charge of the computer or the computer system. (Section 22(1) of this Act) Further a copy of such data may be provided to the owner or the person in charge upon an application for a copy being made to such police offer. (Section 22(2))

Section 23 requires every person to assist and provide information in the course of an investigation under this Act. Section 24 imposes duty towards police officers, experts and any other person or persons involved in any investigation under this Act that they should maintain strict confidentiality in all information acquired by them during the course of their investigation.

However Computer Crimes Act of Sri Lanka has been introduced to a new regime of investigation on computer crimes. Without effective and efficient investigation one cannot enjoy the benefits of their law. Therefore the appointment of experts to assist police officers helps accomplish the goals aimed by this Act.

In a democratic country every person has his own need for rights and they all need to be treating of equally. (Article 12 of the Constitution) Therefore a criminal investigation also should be conducted in such manner to protect the rights of any party involved in this investigation. Our Computer Crimes Act has succeeded in this challenge. The concept of 'experts' in this act ensures that accessing a computer is done by skilled, efficient resources and it guarantees the protection of hardware or software in this issue.

II. FINDINGS

Even though Sri Lanka is not a country which has countless victims affected by computer crimes except by traditional offences, it is our responsibility to take precautionary measures for this issue. When we look at the history of computer crimes of developed countries; it has proved that anything can happen at any time. Although we have a legislative enactment on computer crimes namely Computer Crimes Act of 2007, it only discusses the computer related crimes and hacking offences. But generally a computer crime consists of three components one of which has been left out in our Act namely content related cybercrime, which means where computers together with internet resources are used to distribute illegal data. For example, Internet based pornography, Criminal copy right infringement. Therefore it is important now to think about a legislative enactment on cybercrimes and investigations under the same Act. Further to this content related offences are being addressed through a sense of changes to the Penal Code and other statutory provisions. Still it has created complicated issues and they are in dire need for a separate law. It is important to point out investigations for cybercrime when we discuss investigations under computer crimes act in this paper.

Although there is a few computer crime cases reported in Criminal Investigation Department, to be on a safer zone, our country should update and increase our capacity on cybercrime in this modern technological.

III. RECOMMENDATIONS

Education is the most powerful weapon which you can use to change the world (Nelson Mandela). Accordingly we should educate people regarding this issue as we all know; computer crimes are generally called as White Collar Crimes and layman does not have proper idea about this offence on information technology. The government has to take necessary steps educate people from school children as because these days many school going children have facebook accounts.

As mentioned earlier, although we have proper investigation team with the assistance of experts on computer crimes, lack of laws on cybercrime creates the existing law on investigations powerless. Also it is significant that cybercrime is a tool which can affect national security and economic of a country.

The involvement of technology in Sri Lankan life is rapidly growing and most of the government and private sector institutions function their work through computer based system. The engagement on social media of Sri Lanka is also impressive. According to all these changes even though Sri Lanka is still a developing country, the aspects of technology of citizens have been developed. Therefore now it is time to think about best security on computer crimes and cybercrimes with the help of strong investigation pool.

The expert appointment for investigations under Computer Crimes Act, allows experts from the public sector for appointment. It has narrowed the efficiency of our pool. Regarding the appointment of experts to the investigation team and experts, I would like to point out my view that the above mentioned section is a restriction itself to call upon an efficient pool to work for the task. As we all know there are large numbers of experts in this field working for private sector and I think it is necessary to include them and their assistance when we are in need. Therefore we can establish public and private partnership and get support from them too to strengthen our selves.

The existing public awareness programs on investigation on computer crime are not enough to induce people to report their offences related to Information Technology. In addition to this, the concern of government employees who work in IT field also should avoid negligent errors and maintain secrecy.

For a meaningful investigation of Computer crimes, the legal framework should have components such as Computer Forensics. But very few of us are aware of this terms and benefits. It is not recognized as a formal discipline under our computer crime investigations yet.

Computer Forensics is the process of investigating computer equipments and associated storage media to determine if it has been used in the commission of a crime or for unauthorized activities. I think the understanding of the legal and technical aspects of computer forensics ensure utilization of time and money allocate for investigation purpose. Therefore the need for computer forensics has been increased worldwide.

Generally computer forensics can handle the investigation of computer crimes by performing collecting, documenting and preserving digital evidence to extract useful data and combining them to create a clear picture of the whole crime. Why need for computer forensics in Sri Lanka is, although number of computer usages and computer crimes have been increased in Sri Lanka, the number of experts who have excelled in Law and Technology are very few. And there is no forensics team in Sri Lanka to investigate crimes. It is one of the reasons for loopholes in identifying criminals in computer crimes and succeeding in the respective cases.

For now a specialized digital forensic lab is being maintained by the University Of Colombo School Of Computing. But the framework for the analysis of forensic evidence is in need. Further we have to concern on Computer related crimes to focus computer crimes on the internet and investigations regarding them.

Still investigation of Computer crimes in Sri Lanka, has not recognized proper ways to handle computer crimes such as, intrusions, sex offenders on the internet and cyber stalking. Firstly, gaining entry to a computer without the owner giving consent is called intrusion. Adware, hijacking, spam, spyware, phishing and virus, worm and cookies are examples for intruders. Investigating computer intrusions normally involves a large amount of digital evidence, but Sri Lanka does not have a determined admissibility of digital evidence in practical.

During the investigations on sex offenders and cyber stalking, it has been proved that digital evidence itself is not enough to declare reasonableness and justice. It is important to investigate the behavior of an offender. Victimology can help to accomplish this task. Victimology means an investigation and study of victim characteristics.

IV. CONCLUSION

Even though the act has introduced the team “experts” to challenge the investigations under this Act practically, the real challenge is that the common concern of experts in giving evidence and exposing them to cross examination in a court of law. It creates many on efficient and effective experts to show reluctance to be an expert under this Act. In addition to this, our procedural law also does not facilitate submitting affidavit evidences on sensitive investigations.

Although the admissibility of electronic or computer based evidence is accepted in laws (Evidence (Special Provisions) Act 14 of 1995) the admissibility is subject to criteria. Further there are few laws yet to be amended or reviewed. For example, the relevancy of Electronic Transaction Act (19 of 2006) on investigations under Computer Crimes Act. Our Act is silent on this kind of matters.

Before I conclude this paper, I like to mention a piece of news which came across stating that a group of hacker cracked in to websites of the Media Centre for National Security (MCNS), North Central Provincial Council, the Ports Authority, Board of Investment, Nelum Pokuna Theatre, Justice Ministry, Immigration Department and Probation Department. (Statement of Information Technology Minister - Sunday March 2013, Colombo Page News Desk, Sri Lanka) The question here is if these kinds of incidents or beyond these occur in future how should those cases be treated or investigated?

Law makers and relevant authorities have a great task ahead of them for the formation of cyber laws and investigations for us. It is time to take seriousness of computer crimes. Computer crime offence can happen from a room to another room or a room to a country and it can cause internal harm or external harm. It may attack an individual or the interests of a country.

If you go through the number of computer crime cases in the past few years after the enactment of the act, from 2007 to 2011 there are 178 reported cases. (Presentation of M.K.D. Wijaya Amarasinghe - Director/ Criminal Investigation Department) It shows the possibility of increasing the number of computer crime cases in future. As long as there is a system in law to punish the wrong doers, and there is public awareness of this type of crimes, we can ensure the protection from Computer crimes.

I think it should better to have experts for an investigation from outside of country depending on the ratio of crime and nature of need. The existing Computer Crimes Act of Sri Lanka does not cover Computer related (Cyber) Crimes Investigations. It means existing legislation may not be suitable or adequate for investigations under computer crimes. Therefore new laws are required in order to facilitate investigations for cybercrimes.

REFERENCES

Amarasinghe MKDW (2013). "Investigations conducted under Computer Crimes Act No 24 of 2007",Available:http://www.coe.int/t/dghl/ cooperation/economiccrime/cybercrime/cy_activity_Sri_Lanka_apr_11/session_7_W_Amarasinghe_Computercrime_Act_of_SriLanka.pdf

Code of Criminal Procedure Act No 15 of 1979.

Computer Crimes Act of 2007

Computer Crimes and Cybercrimes: Is there a difference?"<http://www.techsavvy.or.ke/magazine/2012/06/05/computer_crimes_and-cyber_crimes_is_there_a_difference/#sthash_yu6024Ld.dpuf.> [Accessed 5th August 2013]

Electronic Transaction Act No 19 of 2006

Evidence (Special Provisions Act)

Fernando Jayantha, "Cybercrime legislation- Sri Lankan Upate" –<http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/Reports_Presentations/2079if09pres_SriLanka_Jayantha.paf> [Accessed 5th August 2013]

Furnell S (2002). Cyber-crime: Vandalizing the Information Society. London: Pearson Education Ltd.

KalingaIndatissa (2008). Law Relating to Computer Crimes and A Commentary on the Computer Crimes Act No 24 of 2007, Sri Lanka.

Penal Code of Sri Lanka 1885

Sri Lanka to amend Computer Crimes Act<http://www.colombopage.com/archieve_13A/mario_1362925419jR.php> Accessed 5th August 2013

BIOGRAPHY OF THE AUTHOR

Author is a lecturer at Department of Legal Studies, The Open University, and Sri Lanka. She is a Law graduate from University of Colombo, Sri Lanka and she has her LL.B with honours. Before starting her career as a lecturer and lawyer, as an undergraduate she served for UNDP – Equal Access to Justice Project, Law and Society Trust and Centre for Housing Rights and Eviction, Sri Lanka as a research assistant and legal trainee. Currently she is reading for her masters on Human Resource Management at University of Colombo. Her research interests include Commercial Law, Information Technology Law and Human Rights Law. Currently, she works on the component of "Leadership and personality development of children"- Child Rights based an action research project of "Developing Children as Change Agents in Community Development" at Institute for Gender and Development Studies.