AN EVALUATION OF THE LEGAL FRAMEWORK OF CYBER-CRIMES IN SRI LANKA

DAMITHRI KODITHUWAKKU

Attorney-at-law,
LL.B(Hons)(United Kingdom)

Technical infrastructure of today's world highly depends on internet. Social, political, business, education, health, leisure and entertainment, media practices of people are highly influenced with the rapid development of Information technology. Internet has become the basic tool which facilitates the global communication and all are provided with increased opportunities in the global cyber arena.[1] With the development of Information technology to cater human needs using virtual dimension, ordinary services have converted into electronic forms and the E-Banking, E-Business, Communication, Education and E-Governance fields are highly utilised. Despite the all advantages of IT developments number of crimes relating to IT have been increasing and more people become vulnerable each day.

With the rapid development in technology and the internet, new types of crimes and new means of committing traditional crimes have been discovered.

> "*The computer is rapidly increasing society's dependence upon it, with the result that society becomes progressively more vulnerable to computer malfunction, whether accidental or deliberately induced, and to computer manipulation and white-color law-breaking*".[2]

With the emerging use of information technology and computers related crimes have become a global concern. Gradually almost all the electronic devices including smartphones, tablets, watches, health related devices would have a distinct Internet Protocol (IP) address and with the facility to connected to the internet and as a result of that vulnerability of users get increased and attacks on these devises could damage the core functions of the society.[3] As a result of storage of confidential information, privacy and data protection has

[1] KennedyD Gunawardana , 'Current Status of Information Technology And Its Issues in Sri Lanka ' [September - December, 2007] Vol 15(No3)International Journal of The Computer, the Internet and Management <https://pdfs.semanticscholar.org/d735/e0199919d65bd3785c28da449cc6f3f33e43.pdf> accessed 4 August 2019

[2] C. G. Weeramantry, Justice Without Frontiers: Furthering Human Rights, (First published 1997, Published online by Cambridge University Press: 27 February 2017) 259

[3] Jayantha Fernando, 'THE IMPACT OF THE BUDAPEST CYBERCRIME CONVENTION ON SRI LANKAN LEGAL SYSTEM'[2016]

become a major concern as computers are not only targeted for crime but are also important instruments used in the commission of other offences.

Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.[4] The Evidence(Special Provisions) Act[5], the Information and Communication Technology[6], the Payment and Settlement Systems Act[7], the Electronic Transactions Act[8], the Payment Devices Frauds Act[9] and the Computer Crime Act[10] are the main pieces of legislations which governs the legal regime in the area of Information Technology in Sri Lanka. The term "cyber-crime" is used to cover a wide variety of criminal conduct and include a broad range of different offences. One approach can be found in the Convention on Cybercrime, which distinguishes between four different types of offences: offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences and copyright-related offences.[11]

In Sri Lanka, Computer Crimes Act No. 24 of 2007 primarily addresses computer-related crimes and hacking offences. In this Act, computer crime is a term used to identify all crimes frauds that are connected with or related to computer and Information and Communication Technology Act No.27 of 2003information technology. This Act covers a broad range of offences which are common offences identified and recognized internationally as well. Recognising the nature of computer crimes which are committed disregarding boundaries under the Section 2 of the Computer Crime Act courts have a wide jurisdiction to attend the matters irrespective of whether the person resides, the crime was committed or the damage was caused a person or corporation within or outside Sri Lanka.[12] In line with Article 22 of the Budapest convention, Computer Crime Act covers wide range of application without considering the geographical boarders and nationality.[13] Section 27 enables the extradition of cyber criminals among the states.[14] However, above said provisions will not effectively function without the international cooperation among the states, one state

[4] Gade, Nikhita Reddy & Reddy, A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Ugander. (2014).
[5] The Evidence(Special Provisions) Act No.14 of 1995
[6] Information and Communication Technology Act No.27 of 2003
[7] Payment and Settlement Systems Act No.28 of 2005
[8] Electronic Transactions Act No.19 of 2006
[9] Payment Devices Frauds Act No.30 of 2006
[10] Computer Crime Act No.24 of 2007
[11] Marco Gercke, Understanding cybercrime: phenomena, challenges and legal (ITU Telecommunication Development Bureau) < www.itu.int/ITU-D/cyb/cybersecurity/legislation.html> Accessed on 5th August
[12] Computer Crime Act No.24 of 2007 , Section 2,
[13] Computer Crime Act No.24 of 2007 Section 2,
[14] Computer Crime Act No.24 of 2007, Section 27.

can't solely fight against the computer crimes.[15]

In Section 3 to Section 10, the Act describes the key substantive offences under Computer Crime Act such as Hacking (illegal access)[16] , Cracking[17], unlawful modification[18], offences against national security[19], dealing with unlawfully obtained data[20], illegal interception of data[21], using illegal devices[22] and unauthorized disclosure of information[23] which are adequately consistence with the Budapest Convention under the heading of computer-integrity offences[24].

There are no laws or policies to ensure cyber security, privacy or data protection in Sri Lanka. Although hacking and some other activities are offences under the Computer Crime Act, a remedy can't be offered to a citizen if his or her sensitive data is withheld. This has a direct impact on our trade because some countries are reluctant to enter into transactions with us due to the lack of security in these on-line transactions. If a country wants to actually enter into international trade and commerce, then there must be directives and policies to protect data.

In Sri Lanka, there is a challenge in preventing cyber-crime. The growth of network-based crime has raised difficult issue in respect of appropriate balance between the needs of those investigating and prosecuting such crime, and the rights of users of such networks, so there is a need to empower the coordination process. Prosecutors, investigators, and Judges need to work in coordinating manner and experienced investigators need to be trained properly in order to deal with cyber-crime. Awareness in new media literacy and information technology is one way of minimizing cyber-crime. Further, Sri Lankan legal system needs to be reviewed in order to identify areas which need further modifications.

Computer Crime Act introduced new procedures in addition to the ordinary criminal procedures and every offences under this Act are cognizable offences[25]. Further a significant arrangement is that, government can appoint a panel of experts to assist police officers.[26] A panel of experts shall be appointed in order to assist the police officers in the investigation process. In the process of investigating the police officers and the experts are required to

[15] Jonathan Clough, A World Of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation, Monash University Law Review2011 (Vol 40, No 3)
[16] Computer Crimes Act No. 24 of 2007 Section 3.
[17] Computer Crimes Act No. 24 of 2007 Section 4
[18] Computer Crimes Act No. 24 of 2007 Section 5
[19] Computer Crimes Act No. 24 of 2007 Section 6
[20] Computer Crimes Act No. 24 of 2007, Section 7
[21] Computer Crimes Act No. 24 of 2007, Section 8
[22] Computer Crimes Act No. 24 of 2007, Section 9
[23] Computer Crimes Act No. 24 of 2007, Section 10
[24] Convention on Cybercrime, Budapest, 23 November 2001
[25] Computer Crimes Act No. 24 of 2007 Section 21
[26] Computer Crimes Act No. 24 of 2007 Section 17

consider the protection of information and rights of the individuals.

Computer Crime Act complies with the Budapest Convention (Art 16-21), and provides special power to the investigation officers including the power of search and seizure which includes the laws for interception and real time collection of traffic data[27], and the request to preserve information[28]. However, some procedures have to be strengthened based on international standards. Compiles with Article 15 of the Budapest convention, Computer Crime Act strives to ensure the right to privacy of the victims[29] however when it comes to Sri Lankan contest right to privacy of victims cannot be ensured in the investigation and prosecution process.

Furthermore, for the purpose of effective enforcement Sri Lanka has established the computer crime division of police department and computer emergence response team(CERT). Moreover, the Computer Crime Act enables mutual assistance of states for investigation and prosecution of cybercrime through the Criminal matters Act 2002.[30] Furthermore, Sri Lanka's accession to the Budapest convention which leads to obtain mutual legal assistance from other member states, through that Sri Lanka can combat against the computer crime.[31]

In 2015, as the first country from South Asian region Sri Lanka acceded to the Budapest Convention. Though the Computer crime Act was enacted before the said accession, the majority of the provisions were in compliance with the Budapest Convention. Some provisions of the Convention were not covered by the Computer Crimes Act such as Child Pornography[32]. However the Sri Lankan Penal code has provisions to address this, however it may not adequate enough to prosecute these crimes when it is committed using Internet.[33]

A major challenge in the existing legal framework is that the Computer Crimes Act has failed to identify some of the most common cyber-crime offences, such as Illegal gambling, cyber-squatting, hate speech and statements promoting racism, cyber defamation, identity theft, cyber bullying and cyber stalking making it difficult take precautions against such offences.[34] The term computer was not defined adequately in the Act and with the limited elements of the offences such as

[27] Computer Crimes Act No. 24 of 2007 Section 18
[28] Computer Crimes Act No. 24 of 2007 Section 19
[29] Computer Crimes Act No. 24 of 2007 Section 24
[30] Computer Crimes Act No. 24 of 2007 Section 35.
[31] Convention on Cybercrime, NOVEMBER 13, 2018 The Lakshman Kadirgamar Institute (LKI) < https://www.lki.lk/publication/convention-on-cybercrime/> Accsesed on 5th August 2019

[32] Article 9 of the Budapest Convention
[33] Sri Lankan penal code section 286A
[34] Selvaras Janaha, 'Has Sri Lanka Worked Out Effective Ways of Fighting Computer Crime?' (Open University of Sri Lanka 2013) < http://www.kdu.ac.lk/proceedings/irc2013/2013/l006.pdf >Acsessed on 5th August 2019

unauthorized access can be seen as inadequate areas of the Act.[35]

As a developing country Sri Lanka can always take lessons from other developed jurisdictions such as USA, UK, Australia and even from India as they have taken some different approaches in recognizing new types of cyber-crimes. Australia has recognised online illegal gambling as a criminal offence by the Interactive Gambling Act 2001. Further, USA in order to prevent cyber-squatting, abusive registration and use of the distinctive trademarks of others as internet domain names, with the intention of earning profits through the goodwill associated with those trademarks has introduced anti-cybersquatting Consumer Protection Act of 1999.[36] In the UK, hate speech is recognised as an offence under many statutes and under the Communications Act 2003, many offenders have been convicted for the publication of statements promoting hatred in social media.[37] Section 66A of the Information Technology Act 2008 of India, provides the law governing a wide range of common cyber-crimes. It provides the punishment for sending offensive messages through communication services and the provision is so drafted to provide for the punishment of cyber-bullying, cyber-stalking offenders. The above examples from other jurisdictions effectively illustrates how those jurisdictions have stepped towards implementation of an effective legal framework by identification of common cyber-offences as criminal offences.

The "Access" is a commonly used term in ICT law, especially in relation to cyber-crimes. Yet, the term is not interpreted in the statutes. In this case, the Information Technology Act 2008 of India provides an interpretation to the term "access". Accordingly, "access" means; "gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network"[38] The element of "unauthorised access to commit an offence" is the given term as the *actus reus* for several offences in Sri Lankan Computer Crime Act. However, as there are various types of offences which come under cyber-crimes it may be difficult to take each and every offence under this element as in order to identify as a cyber-crime, as there are several offences which can be done with lawful access. The 2008 amendment to the Information Technology Act 2000 of India has introduced offences such as sending offensive messages, spam, identity theft,

[35] Dr Thusitha ABEYSEKARA and Samindika ELKADUWE, 'A Game of Thrones': Law V Technology: A Critical Study on the Computer Crimes Legislation in Sri Lanka, Second International Conference on Interdisciplinary Legal Studies 2015(ISBN-978-0-9939889-3-6)page28

[36] Martin Samson, 'The Anti-cybersquatting Consumer Protection Act: Key Information - Internet Library Of Law And Court Decisions' (*Internetlibrary.com*, 2019) <http://www.internetlibrary.com/publications/anticybsquattSamson9-05_art.cfm> accessed 28 August 2019

[37] 'Everything You Need To Know About Cyberbullying And How To Stop It' <http://www.thebetterindia.com/71909/cyberbullying-it-act-2000-cyber-law-in-india/> accessed 28 August 2019

[38] Information Technology Act 2008, section 2(1)(a)

cheating by personation, and violation of privacy rather than placing them under the unauthorized access.[39] A further challenge which is faced by the law enforcement authorities is that the offences under the Computer Crime Act are entirely based on the principle of unlawful access. Accordingly, the Act fails to cover situations where information/data is obtained by lawful access, but are consequently misused for unauthorized purposes; for example, Cookies issues.

Cyber defamation is one of most common type of cyber-crime globally as well as in Sri Lanka. Since, defamation is not a criminal offence, the Police or any other law enforcement officials are unable to prevent such crimes. It is evidential that in social media platforms people are daily subject to cyber defamation.

One of the major challenges faced by the Sri Lankan legal system is the lack of reporting of cyber-crimes. A main cause behind lack of reporting is that the victims fear that their data might get destroyed or they might lose the confidentiality of their private data.[40] Another one of the main drawbacks in the existing legal framework on cyber-crimes is that lack of case law. There are no reported case law on cyber-crimes and very limited numbers of cases are taken before the courts which make impossible to develop the legal framework relating to cyber-crimes.

Further, most of the individuals are not aware that they are victims of cyber-crimes and victims are not aware that there are legal remedies which they can seek out to mitigate the harm. Therefore, only a few numbers of cases are reported to the courts and the judges don't get an opportunity to administer law against the offenders.[41]

Sri Lanka is actually a pioneer in terms of ratifying international and regional conventions related to ICT Law. However, ironically, when it comes to adopting them and **implementing** them, we are lagging behind. There are special and simplified procedures provided by the law in relation to computer crimes where the police can even obtain the help of experts who hold proper qualifications. They can perform several tasks without even receiving a court order. However, none of this is implemented. It is necessary to research on how other countries have enforced their laws and integrated the culture of responsibly using the internet and digital devices and educate our society.

---

[39] Lionel Faleiro, IT Act 2000 – Penalties, Offences With Case Studies, June 24, 2014 < https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/> Accessed on 10th August 2019

[40] Marco Gercke, Understanding cybercrime: phenomena, challenges and legal (ITU Telecommunication Development Bureau) < www.itu.int/ITU-D/cyb/cybersecurity/legislation.html> Accessed on 5th August

[41] Vishni Lakna Ganepola, Effectiveness Of The Existing Legal Framework Governing Cyber-Crimes In Sri Lanka

Although the Computer Crimes Act seems to be adequate in comparison to the Budapest convention, as it provides for identification of crimes, identifies a wide jurisdiction and provides an investigation procedure, the extent of implementation of the provisions of Computer Crime Act cannot be seen as a result of various reasons such as lack of reporting, lack of investigation officers who has adequate knowledge to deal with highly skilled cyber criminals and lack of investigation equipment. Further, social media flat forms such as Facebook are unwilling to provide information such as IP addresses of users and therefore it is necessary to take steps coordinating with those international corporations.

Sri Lanka needs to enact laws to streamline the existing legal framework on cyber-crimes with the international standards such as identifying new types of offences, introduce Data Protection Act and Reform defamation laws and introduce cyber defamation laws. In achieving these developments Sri Lanka can use International Conventions such as Budapest Convention, developments of other jurisdictions as guidelines and can seek assistant from them. Awareness about existing legal framework is much important since victims of cyber-crimes need to be encouraged to report such crimes which will eventually contribute towards the development of legal framework relating to cyber-crimes. .