THE LEGAL REGIME OF CYBER CRIMES IN SRI LANKA

J. G. Sadini Rumeshika*

Today, you and I live in an age where electronic devices and computers play a significant role in the advancement of our lives. While having an impact on the various aspects of our daily practices, information technology has made a difference in the fields of education, commerce, business, communications, governance and banking. However, the use of computers and electronic devices has not been very healthy in the recent past and present. These equipmentS are very often used by criminals to commit offences and therefore, the need for a strong framework of laws was identified by the legislature in order to regulate cyber discipline. This legal article will first focus on how the law relating to information and communication technology has been developed and amended to suit the nature of present day cybercrime offences. Next, apart from its development, this article will examine the procedural law related to submission of electronic and computer evidence within the jurisdiction of Sri Lanka. Finally, an insight to the recently developed legislature and challenges posed in implementing such legislature will be discussed in order to bring to the reader's attention that the legal framework of ICT Law in Sri Lanka requires a fundamental update.

Cyber-Crimes and Cyber Law

Various approaches have been adopted in recent times to develop an accurate definition for both terms cyber-crimes and computer crimes (Australian Institute for Criminology; 2005). At the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed (10th UN Congress on the Prevention of Crime and the Treatment of Offenders; 2000). Cybercrime (computer crime) in a narrow sense covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrimes in a broader sense (computer-related crimes) cover any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network (Kumar; 2009). Cyber law can be defined as any law that applies to the internet and internet-related technologies and is one of the latest areas of the legal systems. It still seen to be expanding pertaining to the reason that internet technology develops at a very rapid rate and it is important to provide legal protection to those using the internet. Although Sri Lanka is still at a tender age with the advancement in technology, digital technologies have long evolved into

* Attorney-at-Law

ISSN 1800-055X Vol. Iv

fundamental social infrastructure in Sri Lanka. This wide scope of cyber-crimes include email spoofing, forgery, cyber defamation, cyber stalking and phishing, identity theft, hacking, spreading hate and inciting terrorism, distributing child pornography and grooming: making sexual advances to minors (Journal in Computer Virology; 2006).

Sri Lanka's Position prior to 1995

The absence of distinct legal provisions to deal with computer and electronic evidence created difficulties with regard to the reception of such evidence in Sri Lanka. In the case of ***Benwell vs. Republic of Sri Lanka*** *(1978-79) 2 SLR 194*, which related to the extradition of an Australian citizen, it was decided that *"Computer Evidence is a category in its own; it is neither direct evidence nor derivative evidence. And such evidence is not admissible under Section 34 of the Evidence Ordinance or any other provision of the Ordinance"*. This case identified that computer evidence was a unique category which required special statutory provisions for the reception of computer related evidence.

Similarly, the Hearsay Rule which is accepted under the Evidence Ordinance was also a hindrance to the reception of computer evidence. In accordance with the ratio decidendi of the case ***Regina v Wood*** *(1982) 76 Cr App R 23*, the said rule required that each and every person who contributed to their creation must testify. However, as computer generated documents are programs designed and based on data entered by one or more persons, the above requirement was impractical to fulfill. Therefore, the absence of necessary provisions in the Evidence Ordinance with regard to the reception of electronic and computer evidence was an issue problematic in nature.

Legislative Enactments related to ICT in Sri Lanka

The matter discussed above was then successfully addressed with the introduction of legal provisions from 1995, which catered to the needs of the reception of electronic and computer evidence in Sri Lanka. The Acts which have been enacted are The Evidence (Special Provisions) Act No. 14 of 1995, the Information and Communication Technology Act No. 27 of 2003, the Payment and Settlement Systems Act No. 28 of 2005, the Electronic Transactions Act No. 19 of 2006, the Payment Devices Fraud Act No. 30 of 2006 and the Computer Crime Act No. 24 of 2007. Furthermore, the Telecommunications Act No. 25 of 1991 and Act No. 27 of 1996 were enacted introducing the Telecommunications Regulatory Commission of Sri Lanka (TRCSL).

"*As a result of the enactment of the Information Technology Act No. 27 of 2003, the Information and Communication Technology Agency (ICTA) of Sri Lanka was set up by the Government of Sri Lanka to meet the objectives of the Act. The main objective of the Evidence (Special Provisions) Act No. 14 of 1995 was to provide for the admissibility of electronic and computer evidence in civil and criminal proceedings. One of the objectives of the Payment and Settlement Systems Act No. 28 of 2005 was to facilitate electronic*

ISSN 1800-055X Vol. Iv

presentment of cheques. The purpose of the Electronic Transactions ActNo. 19 of 2006 was to recognize and facilitate the formation of contracts, the creation and exchange of data, messages, electronic documents and other forms of electronic communications in Sri Lanka. The Computer Crimes Act No. 24 of 2007 was enacted to provide for the identification of computer crimes and to provide procedures to prevent such crimes." (Abeyratne; 2008)

Key Legal Provisions under the Computer Crimes Act No. 24 of 2007

Since the Penal Code of Sri Lanka deals with traditional offences, a new system of regulations was required for the governance of crimes related to computers. This resulted in the enacting of the Computer Crimes Bill (LD-O72/2000) on 8th May 2007and its operation was effective from the 15th July 2008 as the Computer Crimes Act No. 24 of 2007 (Fernando; 2016). This legislation is the result of contributions from CINTEC Committee on Law & Computers which lasted from 1995 to 2000. It furnished for the loopholes that the Penal Code faced when dealing with computer and electronic evidence. The Computer Crimes Act has laid down the procedure to identify computer crimes, the method of investigating them and the prevention of such crimes.

Part I of the Computer Crimes Act explains the offences relating to cyber-crimes and the salient features of the Act are discussed from Section 2 to Section 10.

Section 2 stipulates the scope of this Act and it applies to a person who, while outside or inside Sri Lanka, commits an offence (loss or damage to the State or person resident in or outside Sri Lanka) affecting a computer, computer system, information or data storage system which was inside or outside of Sri Lanka at the material time.

Above mentioned offences may be of a wide range and the Computer Crimes Act of Sri Lanka narrows down these offences to the following categories(Abeyratne; 2008):

1. Computer related offences – where the accused uses a computer or network as a tool to commit the offence.
2. Computer integrated offences – where the accused commits offences through a computer or computer system or programs such as hacking and modification by viruses.

Section 3 criminalises unauthorised access to a computer or any information held in a computer where the accused intentionally secures any programme or data with the knowledge that his conduct was unlawful. This offence is known as Computer Hacking which is done through viruses, cookies and web bugs, web linking, web framing and spamming. Section 4 constitutes the same ingredients as in Section 3 with the additional element that such unauthorised access was gained with the intention to commit an offence. This offence is known as Computer Cracking and extends to sniffing and phishing. Section 5 criminalises the offences of causing a computer to perform a function without lawful authority. Prosecution has to satisfy that the accused caused a computer to

ISSN 1800-055X Vol. Iv

perform a function, intentionally and without lawful authority and that he had knowledge to believe that such function would cause unauthorised modification or damage to any computer, computer system or computer programme. This offence is known an unauthorised modification and may be caused by impairing the operation of a computer, destroying, deleting, corrupting, adding or altering data or information held in a computer and introducing a computer programme to cause malfunction a computer.

Section 6 deals with offences intentionally committed by an accused, by causing a computer to perform a function, which eventually results in danger or imminent danger to the national security, national economy or public order of the country. Section 7 penalizes buying, receiving, retaining, selling, downloading, uploading, copying or acquiring of unlawfully obtained information. Section 8 deals with the offence of illegal interception of any subscriber information or traffic data to or from or within a computer, knowingly or without lawful authority. Section 9 deals with the offence of producing, selling, processing, importing, exporting, distributing or making available any computer or computer programme, a password, access code that is capable of being accessed with the intent that such information be used for the committing of an offence. Finally, Section 10 deals with the offence of unauthorised disclosure of information where a person who is entrusted with information which enables him to gain access to any service provided by the computer, discloses such information without expressed authority to do so.

The offences discussed above can be found compatible with those offences set in the Council of Europe Convection on Cyber Crime and these prove to be common offences identified and recognized internationally as well.

Investigation and Security Strategy in Sri Lanka

Part II of the Computer Crimes Act provides legal provisions for the purpose of investigations related to the offences discussed in Part I of the Act. Pursuant to Section 16 of the Computer Crimes Act 2007, all offences under this Act are cognizable. Therefore, according to Section 15 of the Act, such offences shall be investigated, tried or dealt with the legal provisions set out in the Code of Criminal Procedure Act No. 19 of 1979 unless otherwise provided under the Computer Crimes Act.

As provided by Section 17, the Minister in charge of the subject of Science and Technology shall appoint a team of experts in accordance with the qualifications, experience and remuneration set out in the Computer Crimes Act. This panel of experts called upon to assist police officers shall have the power under Section 17(4) of the Act to enter any premise along with any police officer not below the rank of a sub inspector, to access any information system, computer or computer system, perform any function, require any person to disclose any traffic data, orally examine a person and do any such other things that may be reasonably required for the purpose of this Act. Further, these officials are vested with power under Section 18 of the Act to search and seize any

ISSN 1800-055X Vol. Iv

subscriber information and/or traffic data, intercept any wire or electronic communication with a warrant. Furthermore, if preservation of information requires the purposes of investigation, the experts or police officers have power under Section 21 to arrest, search and seize any information within any premises without a warrant in the course of investigation.

These legal provisions provide the necessary steps to be taken to accelerate the investigations of computer crimes in the interest of justice.

The Evidence (Special Provisions) Act No. 14 of 1995 provides for the admission of two types of evidence namely, Contemporaneous Recordings and Computer Evidence contained in statements produced by computers in civil and criminal proceedings. Some of the main concerns that parties to such a case would have can be summarized to the following:

1. Will it be permissible to adduce that evidence at the trial?
2. What procedural steps should be followed for adducing such evidence?
3. To what extent and by what methods may such evidence be open to challenge?
4. How cogent will that evidence be?

In addressing the above questions, the Evidence (Special Provisions) Act No. 14 of 1995 enables a party to produce "in any proceeding where direct oral evidence of a fact would be admissible, any statement produced by a computer and tending to establish that fact" provided it is shown that

a. The statement in the form that it was produced is capable of being perceived by the senses;
b. At all material times the computer producing the statement was operating properly; and
c. The information supplied to the computer was accurate.

As decided in the case of ***Abu Bakr v The Queen*** *54 NLR 566* the precondition that the statement produced by the computer must be perceived by senses is however, not an absolute one. In ***Kularatne and Another v Rajapakse*** *(1985) 1 SLR 24,* it held that a transcript, translation, conversion or transformation which is intelligible and is capable of being perceived by the senses may be admitted in evidence where the statement made by a computer cannot be played, displayed or reproduced in its original form. As identified by Section 69 of Police and Criminal Evidence Act 1984 of United Kingdom, another vital element is to ensure that the information supplied to the computer was accurate because in some cases, failure to adopt procedures for safeguarding the accuracy and integrity of computerized records may result in court or judge refusing to recognize the authenticity or admissibility of data derived from them.

Legality on Electronic Transactions

While traditional commercial transactions take the format of paper-based medium, electronic commerce or e-commerce involves transactions that take place over the internet. Under E-commerce, parties have the ability of entering into contracts from any part of the world, even in the absence of a

ISSN 1800-055X Vol. Iv

meeting or a simple telephone conversation. In order to legalize the validity of such electronic transactions, the Electronic Transactions Act No. 19 of 2006 was introduced to the Sri Lankan legal framework on ICT. This Act facilitates domestic and international e-commerce by eliminating legal barriers and establishing legal certainty; it encourages the use of reliable forms of electronic commerce; it provides for the electronic filling of documents and services and communications with the Government and Private sector; and this Act also promotes public confidence in the authenticity, integrity and reliability of data messages, documents and other types of communications generated electronically. Furthermore, Section 7 of the Electronic Transactions Act of 2006 has enabled the legal recognition of an electronic signature where the following extensions can be interpreted as enforceable electronic signatures: agreements made by e-mails, entering of a Personal Identification Number (PIN) into a bank Automated Teller Machine (ATM), signing of credit or debit slips with a digital pen pad device at the point of sale and signing electronic documents online.

Under the Evidence Ordinance, documents to be produced in court are subject to proof and such proof is achieved where the originals of relevant documents are made available. However, overtaking this requirement under the Evidence Ordinance, the Electronic Transactions Act allows for a strong presumption under Section 21 that the information contained in an electronic data message, document, record or any other type of electronic communication is firstly truthful, secondly made by the person who is purported to have made it and thirdly that the electronic signature or the distinctive identification mark is genuine.

While appreciating the fact that this Act has brought an insight to electronic transactions with validation to online communications; a different dynamic to contracts and freedom to e-transactions, it is also important to note that there are certain restrictions that prevent the application of this Act. According to Section 23, the creation or execution of a will or any testamentary disposition, a license for a telecommunication system issued under Section 17(6) of the Telecommunication Act; a Bill of Exchange defined under Section 3(1) of the Bill of Exchange Ordinance; a Power of Attorney defined under Section2 of the Power of Attorney Ordinance; a Trust defined in the Trust Ordinance excluding constructive, implied and resulting trust; a contract for the sale or conveyance of immovable property and any document, Act or transaction upon the Minister's regulation are excluded from the applicability of the Electronic Transactions Act. A reasonable explanation to such exclusion would be that, for example, the execution of a will or a signing of a Deed of Sale will require the presence of a Notary Public and two witnesses to be present at such time of signing, in accordance with the Prevention of Frauds Ordinance. This requirement would prove to be impractical in the context of an online transaction as the law does not provide for presence of Notary Public and witnesses in an online mode or through any form of communication within the medium of internet. As this situation has posed a challenge on such restrictions, it is also important to note that Sri Lanka is still

ISSN 1800-055X Vol. Iv

experiencing the basic stage of the Electronic Transactions Act and that there has been no legal development for the past 14 years since its origination.

Challenges faced outside the legal framework

Despite the availability of a well-structured legal framework for the governance on offences of cybercrimes, Sri Lanka faces certain challenges and practical issues that remain unsolved up-to-date. These encounters may include the following:

1. Shortage of experts within the country as many professionals lack the required qualifications and experience in the ICT industry.
2. Reluctance of available experts to investigate and give evidence in a court of law as they would be thoroughly cross-examined by the learned opposing counsel.
3. Even though the existing laws provide for the admissibility of computer generated records, such admissibility is subject to several strict criteria, ex: Certificate to prove that the computer was working properly.
4. Shortcomings of the administration of the country such as public awareness of the existence of the Acts and the uses that general public can gain in the event of an offence or infringement of an individual's right.
5. High expenses are to be incurred when training experts and police officers to investigate into ICT related matters.
6. Non-availability or insufficiency of computer forensic laboratories in the country.

Conclusion

Sri Lanka cannot look forward to becoming a developed nation without its citizens being able to use ICT for their personal advantage. While the use of electronic equipment for efficiency is important, protection from cybercrimes has proved to be even more significant as the entire purpose of such commitments would be defeated if cybercrimes could dominate over public confidence. The purpose of enacting the main Acts was to raise the confidence that the general public have in Information Technology services and products and also to govern the admission of electronic and computer evidence in judicial proceedings. While appreciating the prevailing laws, it is equally important to develop and improve certain aspects of the existing law in order to meet the present day challenges, while being based on the fundamental principles of Law of Evidence.

References

Abeyaratne, S. (2008)*Introduction to Information and Communication Technology Law*. Colombo.: Sunil D. B. Abeyratne Publishers.

Fernando, J. (2016).*Cyber-Crime Legislation; A Sri Lankan Update*

Dharmawardena, S.(2015) *Legal Regime of Computer Crimes and Electronic Transaction of Sri Lanka*; Attorney Genral Department Law Journal.

ISSN 1800-055X Vol. Iv

Kumar, A.P. (2009) *Cyber Law, A view to social security*.

Marsoof, S.*Electronic and Computer Evidence in Criminal and Civil Proceedings*.

Acts

The Evidence (Special Provisions) Act No. 14 of 1995

Information and Communication Technology Act No. 27 of 2003

Payment and Settlement Systems Act No. 28 of 2005

Electronic Transactions Act No. 19 of 2006

Payment Devices Fraud Act No. 30 of 2006

Computer Crime Act No. 24 of 2007

Telecommunications Act No. 25 of 1991 and No. 27 of 1996

Police and Criminal Evidence Act 1984 of United Kingdom

Websites and e-books

Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: www.aic.gov.au/topics/cybercrime/definitions.html

Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at.: www.uncjin.org/Documents/congr10/10e.pdf

Explanatory Report to the Council of Europe Convention on Cybercrime, No. 8; Gordon/Ford, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; Chawki, Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview

Council for Information Technology (CINTEC) replaced by ICT Agency of Sri Lanka the apex ICT Agency of government of Sri Lanka (Information and Communication Technology Act No. 27 of 2003)

https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[1]https://www.upcounsel.com/cyber-law
[1]https://www.sundayobserver.lk/2018/07/22/news-features/alarming-increase-sl-cyber-crime

Cases

Benwell v The Republic (1978-79) 2 SLR 194

Regina v Wood (1982) 76 Cr App R 23

Abu Bakr v The Queen 54 NLR 566

Kularatne and Another v Rajapakse (1985) 1 SLR 24

ISSN 1800-055X Vol. Iv