6.2. Electronic Transactions Act No. 19 of 2006.

The Electronic Transactions Act No. 19 of 2006 is based on the standards established by United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996) and Model Law on Electronic Signatures (2001).

The objectives of the Act as are as follows;

- to facilitate domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty;
- to encourage the use of reliable forms of electronic commerce;
- to facilitate electronic filing of documents with government and to promote efficient delivery of government services by means of reliable forms of electronic communications and
- to promote public confidence in the authenticity, integrity and reliability of data messages and electronic communications. This has ensured that electronic communication is officially and legally accepted as a proper means of communication (emphasis added).

The Act applies to all business and commercial transactions which are electronic in nature, other than those specific areas that have been excluded by Section 23 of the Act, namely, wills or other testamentary dispositions, powers-of-attorney, sale or conveyance of immovable property, trusts (excluding constructive, implied and resulting trusts), Bills of Exchange, telecommunication licences, etc.

Section 3 of the Act gives legal recognition to electronic documents in the form of data messages, electronic records, electronic documents and other communications. The terms “Data Messages”, “electronic document”, “Electronic records” and “Communication” have been defined in Section 26 to give the widest possible connotation so as to legally recognize all forms of electronic transactions and communications.

Section 4 provides for the legality of electronic equivalents to instruments which are required to be in writing, provided that the information contained in a data message, electronic record, electronic document or communication, is accessible for subsequent reference.

Sections 5 and 6 of the Act have a similarity to Articles 8 and 10 of the UNCITRAL Model Law on e-Commerce. Section 5 stipulates the minimum standards that must be fulfilled when information usually required to be presented or retained in its original form, is made available in the electronic format via data messages, electronic records, electronic documents. Section 6 describes the legal standards required to be satisfied when the retention of information under any law are to be satisfied, when such information is retained in electronic form. Therefore, document archiving in electronic or digital form is now legally valid under the Act.

Section 7 provides for the legal recognition of Electronic Signatures. The provisions contained in this Section and the associated definition of "electronic signatures", contained in Section 26, ensures that all technologies relating to electronic signatures would have legal recognition.

Section 8 describes the modalities for the use electronic records and electronic signatures in Government institutions and statutory bodies and the procedures to be followed to give effect to such activities. Section 8(2) gives wide powers to the Minister to promulgate appropriate Regulations to transform manual activities and procedures into an electronic paperless mode by setting guidelines and procedures for such transformations in Government (on the recommendation of the respective Government institution).

The regulation making provisions are wide enough to prescribe the manner or methods of payment of any fee or charges for the filing, creation, retention or issue of any electronic record as well as the control process and procedures required in order to secure confidentiality, authenticity and, or, integrity of electronic documents, records, procurements, transactions or payments. These provisions would significantly help in the facilitation of e-Government activities in Sri Lanka.

Sections 11 to 17 of the Act provides for modalities to engage in electronic forms of contracting, including legal recognition of "offer" and "acceptance" in electronic form, enabling businesses and consumers alike to complete the contractual cycle in the electronic mode. Section 11 specifically states that a contract shall not be denied legal validity or enforceability on the sole ground that it is in electronic form. This section has the effect of affirming the application of traditional rules of contract to the electronic environment.

However, for a contract to be effectively concluded in the electronic mode there must be additional rules to ascertain, for instance whether the offer was indeed sent by the "offeror", or whether the "offeree" received the offer, and to enable contracting parties determine when their offer, or acceptance of the offer, was deemed to have been sent. Sections 12 to 14 of the Act give contracting parties the ability to invoke such rules, when concluding contracts in the electronic form.

Section 18 of the Act empowers the relevant Minister, in consultation with the Minister in charge of the subject of Information and Communication Technology, to designate any Government Department, Public Corporation, Statutory Body, Institution, or authority or any branch or unit thereof as the Certification Authority (CA) for the purposes of the Act, by an order published in the Gazette.

The Powers of the Certification Authority designated under Section 18 is stipulated in Section 19. The outline of powers vested in the Certification Authority under Section 19 appears to be in the nature of a "Root CA" or "National CA" and brings Certification Service Providers (CSPs)

under the control and supervision of the Certification Authority (CA) so designated. The powers also envisage setting criteria for accreditation etc, which are standard setting in nature.

Until a special regime was introduced for the admissibility of the Electronic evidence, through Section 21 of the Electronic Transactions Act, the evidence regime in Sri Lanka was governed by the Evidence Ordinance and the Evidence (Special Provisions) Act of 1994.

The rules of evidence contained in the Sri Lankan Evidence Ordinance were evolved long before the advent of modern electronic communications, and those rules have not always proved adaptable to evidence emanating from such modes of communications. Although the term "document" is defined in the Sri Lankan Evidence Ordinance of 1895 as well as the Indian Evidence Act of 1872 in a rather futuristic way, difficulties have arisen in the proof of an electronic transaction by reason of the necessity to produce the original document in Court. The Evidence Ordinance expressly lays down the general rule that "documents must be proved by primary evidence". The Ordinance also declares that "primary evidence means the document itself produced for the inspection of the court". This is problematic in an electronic environment. But secondary evidence is also admissible under Section 63 of the Evidence Ordinance.

A further obstacle towards the production of electronic evidence in courts is known as the "hearsay" rule. This rule, which has been described as "an instance of application of the 'best "evidence" rule", is not expressly referred to in the Evidence Ordinance, but the whole structure of the Evidence Ordinance is predicated on the basis that hearsay evidence is meant to be excluded in criminal as well as civil proceedings in Courts in Sri Lanka as well as in many other countries, such as India, Malaysia, Singapore etc.

Thus, in *Benwell v Republic of Sri Lanka* [1978-79] 2 Sri L.R. 194 which was a habeas corpus proceeding arising in the context of an application for extradition made by the Australian Government, three computer sheets purporting to be entries of books of accounts maintained in an Australian Bank tendered in terms of Section 34 of the Ceylon Evidence Ordinance, were held to be inadmissible in evidence. Colin Thome J, of the Sri Lankan Supreme Court, in the course of his judgment made the following observation:

> "Computer evidence is in a category of its own. It is neither original evidence nor derivative evidence and in admitting such a document a Court must be satisfied that the document has not been tampered with. Under the law of Sri Lanka computer evidence is not admissible under any section of the Evidence Ordinance and certainly not under Section 34."

Further, in terms of Section 67 of the Sri Lankan Evidence Ordinance18 proof of signature and handwriting of a person alleged to have signed or written a document is required before a document could be used in evidence. As held in a decided case19, Section 67 has been

interpreted to have the effect of requiring proof of signature by reference only to handwritten signatures.

Therefore, under the Evidence Ordinance Signature, handwriting and signing obligations can be proved:-
a) by the evidence of the party who signed or wrote the document
b) by the evidence of someone who saw him sign or write it;
c) by the evidence of someone acquainted with his handwriting
d) by the evidence of an expert who compares the writing with some other writing know to be that of the signatory.
e) By proof of the admission of the writer and through comparison by Court, as provided for in Ordinance

To overcome the aforesaid limitations the Legislature responded by enacting two important pieces of legislation, namely, the Evidence Special Provisions Act No. 14 of 1995 and the Electronic Transactions Act No. 19 of 2006.

Whilst Section 22 of the Electronic Transactions Act of 2006 excludes the application of the Evidence (Special Provisions) Act, No. 14 of 1995, Section 21(1), (2) and (3) of the Electronic Transactions Act provides for a specific regime for the admissibility of any data message, communications, electronic document or electronic record and transactions applicable under the said Act.

The Committee stage amendment, introduced to the Electronic Transactions Act during the course of the proceedings in Parliament on 7th March 2006, expands the scope of admissibility under the Act to cover information contained in data messages, electronic documents, electronic records or other communication. Section 21(2) states that "any information contained in a data message, or any electronic document, electronic record or other communication:
(a) touching any fact in issue or relevant fact; and
(b) compiled, received or obtained during the course of any business, trade or profession or other regularly conducted activity, shall be admissible in any proceedings."

The rebuttable presumption in Section 21(3) of the Act provides that
"The Courts shall, unless the contrary is proved, presume the truth of information contained in a data message or in any electronic document or electronic record or other communication, and in the case of any data message or in any electronic document or electronic record or other communication made by a person, that the data message or in any electronic document or electronic record or other communication was made by the person who is purported to have made it and similarly, shall presume the genuineness of any electronic signature or distinctive identification mark therein".

There are three important presumptions in Section 21(3), which shall apply in all cases "unless the contrary is proved." The first of these presumptions is that, all information contained in any data message, electronic document, electronic record or other communication, is true. This is a deviation from the famous hearsay rule. The second of these presumptions relates to the identity of the maker of an electronic document, and is to the effect that unless the contrary is proved, a court of law will presume that any data message, electronic document, electronic record or other communication was made by the person "who is purported to have made it". The third presumption is to the effect that a court will presume the genuineness of any electronic signature unless the contrary is proved.

Thus, Sections 21(1), (2) and (3) of the Electronic Transactions Act provides for a specific regime for the admissibility of any data message, electronic document, electronic record or Communication under the Act. The Committee stage amendment, introduced during the course of the proceedings in Parliament, expands the scope of admissibility under the Act to cover information contained in data messages, electronic documents and electronic records.

Therefore, in terms of admissibility and proof, the Electronic Transactions Act No. 19 of 2006 has taken a giant leap, in comparison with other similar legislation in the region.

As a consequence to the above, in a landmark order delivered by Honorable K. T. Chitrasiri Judge of the Commercial High Court of Colombo (Presently Hon Justice of the Court of Appeal), photocopies containing screen-shots of Short Message Services (commonly known as "SMS") were allowed to be marked and produced in evidence in a money recovery case.
In this case, Marine Star (Pvt) Ltd., the Plaintiff sought to admit photo copies of several SMS's, copied from the messages received on a mobile phone, to prove admission of liability by the Defendant, Amanda Foods Lanka (Pvt) Ltd. Learned Counsel for the Defendant objected to all those documents being produced in evidence stating that no provision in law is available for the Court to admit the contents of such documents in evidence. However, the learned Judge after consideration of the provisions aforesaid permitted admissibility of the SMS transmissions.

Computer Crimes

The Computer Crimes Act No. 24 of 2007 provides for the identification of computer crimes and stipulates the procedure for the investigation and enforcement of such crimes. The basis of the Computer Crimes Act No. 24 of 2007 is to criminalize attempts at unauthorized access to a computer, computer programme, data or information. It also contains a provision to deal with unauthorized use of computers regardless of whether the offender had authority to access the computer.

In terms of scope and applicability Section 2 stipulates that the Act would apply where:-

(a) A person commits an offence under the Act while being present in Sri Lanka or outside Sri Lanka
(b) The Computer, computer system or information affected, by the act which constitutes an offence under this Act, was at the material time in Sri Lanka or outside Sri Lanka
(c) The facility or service, including computer storage or information processing service, used in the commission of an offence under this Act, was situated in Sri Lanka
(d) The loss or damage is caused within or outside Sri Lanka by the commission of an offence under the Act, to the state or to a person resident in Sri Lanka or outside Sri Lanka.

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. They are:-
(1) Computer Related crimes (where computers are used as a tool for criminal activity such as theft, fraud etc)
(2) Hacking offences – which affects integrity, availability and confidentiality of a computer system or network (also includes the introduction of Viruses, worms etc)

The following are some of the key substantive offences under the Computer Crimes Act

- Section 3 of the Act criminalises the securing of unauthorised access to a computer, or any information held in any computer, with knowledge that the offender had no lawful authority to secure such access.
- Section 4 is an enhanced version of Section 3 and criminalises unauthorised access with the intention of committing another offence under the Computer Crimes Act or any other law.
- Section 5 criminalises activity where any person causes a computer to perform a function which results in an unauthorised modification and damage to a computer, computer system or computer program
- Section 6 deals with economic and national security related offences committed by means of a computer.
- Section 7 criminalises buying, receiving, uploading and down loading information unlawfully obtained from a computer or storage medium.
- Section 8 deals with illegal interception of subscriber information or traffic data or any communication to, from or within a computer
- Section 9 criminalises activity such as producing, selling, importing and exporting and distributing Computer or Computer Program or computer passwords or access codes, which could be used for the purpose of committing offences under the Computer Crimes Act.
- Section 10 deals with unauthorised disclosure of information enabling access to a service.

A closer review of the broad range of offences under the Sri Lankan Computer Crimes Act, outlined above, would demonstrate the level of compatibility it has with the Council of Europe Convention on Cyber Crime, the only Convention on the subject which has received global acceptance.

With respect to Content related Cyber Crime (where Computers together with internet resources are used for copyright infringement and pornography related offences), there is a provision in the Act which enhances the scope of Intellectual Property provisions contained in the Intellectual Property Act 36 of 2003. Further, an Amendment made to the Penal Code in 2006 introduced an offence requiring all persons providing a Computer service like a cyber café etc, to ensure that such a service would not be used for offences relating to sexual abuse of a child. This offence as introduced prior to the Computer crimes Act. An amendment is currently being suggested by the Ministry of Justice to the Obscene Publications Ordinance whereby producing, making available, distributing, transmitting or knowingly possessing child pornographic material would be a criminal offence.

In addition, Sri Lanka also introduced the Payment Devices Frauds Act No. 30 of 2006 to specifically deal with possession and use of unauthorized payment devices. This legislation is couched in the widest possible terms to criminalise behavior where computers or the internet is used to commit offences related to payment devices

Any criminal investigation (under the Computer Crimes Act, Payment Devices Frauds Act or any other law), interferes with the rights of others, where a person could be a subject of an investigation or a related third party or a mere intermediary (such as a network service provider). In a democratic society any such interference must be justifiable and proportionate to the needs of society sought to be protected.

However, the growth of network-based crime has raised difficult issues in respect of the appropriate balance between the needs of those investigating and prosecuting such crime, and the rights of users of such networks. In addition, there are the rights and interests of the network providers, the intermediaries that build and, or, operate the networks and services, through which data is communicated.

These challenges require parties to an enforcement process, namely investigators, prosecutors and judges to work in a coordinated manner. This “necessary co-ordination” is also challenging for Governments because of the lack of expertise to often deal with Cyber Crime. As such Governments have been compelled to rely on expertise outside governments, such as Academia and Business.

This is the experience in Sri Lanka as well. The Sri Lankan Computer Crimes Act as well as the Payment Devices Frauds Act has responded to these enforcement challenges by providing for an

“independent” group of experts to assist Law enforcement agencies in the investigation of Crime under the said statutes. These designated experts are fully empowered and given protection under the legislation. The introduction of the concept of an “experts” in these Acts is to ensure that accessing of a computer is done only by skilled resources, capable of performing an efficient detection while at the same time ensuring that the computer hardware and software is not damaged.

Safeguards have also been built in order to protect the businesses and Computer systems that are being investigated. This is to provide the “comfort” measures for organizations and individuals to Report Crimes committed under the Payment Devices Frauds Act as well as the Computer Crimes Act.

The Act creates offences for unauthorized modification, alteration or deletion of information and denial of access, which makes it an offence for any person to program the computer in such a manner so as to prevent authorized persons from obtaining access. Other offences sought to be created under the proposed Act include causing damage or harm to the computer by the introduction of viruses and logic bombs etc, unauthorized copying of information, unauthorized use of computer service and interception of a computer programme, data or information while it is been transmitted from one computer to another.

The Act introduces a new regime for the investigation of offences. Provisions have been made in the Act to designate a panel of ‘Experts’ to assist the Police in the investigation of computer crime offences.

Data Protection

Data protection rules have become an increasingly important legal regime in an information age where personal data has become a significant asset of many companies, especially those operating over the Internet. However, in a connected global economy, national data protection rules can be easily circumvented and protections granted to the citizens lost as data is transferred out of the jurisdiction. In an attempt to prevent such circumvention, the EU data protection regime contains provisions controlling the transfer of personal data to non-EU countries, such as Sri Lanka.

At present the Government is pursuing a policy based on the adoption of a Data Protection Code of Practice, encompassing the private sector, with the possibility of the code being placed on a statutory footing through regulations issued under the Information and Communication Technology Act of 2003. As such, this approach can be seen as self- or co-regulatory approach.