"e-ENABLING LEGISLATION" A CATALYST FOR ICT BASED BANKING AND FINANCIAL SECTOR GROWTH IN SRI LANKA

By Jayantha Fernando[1]
Program Director / Legal Advisor, ICTA

1. Introduction

Over the years the Internet has grown to such proportions that one the "pioneers of the Internet" Dr Vint Cerf once stated that it had "outgrown its original scope and had become an international phenomenon"[2] . This has resulted in a new era of globalization and today we are witnessing the steady growth of Information and Communication Technology (ICT) based activity even in the financial sector.

Banks and Financial Institutions in Sri Lanka have been at the forefront in the deployment of ICT based products and services to provide better services to their customers and consumers. The financial sector has the potential to take off into greater heights in the post conflict era and transform Sri Lanka into a "*Financial Hub*", provided that the entire sector gears itself forward by leveraging on the potentials of Information and Communication Technologies (ICTs) and enter into a new era in the delivery of electronic based financial services.

In a transition towards an electronic based or paperless financial system, doubts and legal uncertainty may prevail in connection with the validity of the services provided through electronic means and whether such transactions could be admissible in courts. In addition questions may be raised in connection with the validity of technological measures, such as Electronic Signatures, which are used to ensure greater integrity, authenticity and security to the banking and financial transactions, effected through the electronic channel and what remedies are available to effectively deal with offenders who try to abuse systems as well as the security measures.

This article addresses some of these fundamental issues, with specific reference to Sri Lankan legislation, most notably the Electronic Transactions Act No. 19 of 2006. Whilst the article would also provide a glimpse of some of the legislative changes, which helped transform the Banking Sector into an ICT based regime, the article would also provide a brief overview of the Computer Crimes Act No. 24 of 2007 as well as the policy approach behind the proposed Data Protection Code of Practice for Sri Lanka.

[1] Jfdo@icta.lk & Jfdo@sltnet.lk

[2] "*Who Controls the Internet – Illusions of a Borderless World*", Goldsmith & Wu, Oxford University Press (2006), Pg

2. Electronic Transactions Act

The Electronic Transactions Act No. 19 of 2006 of Sri Lanka was enacted by Parliament on 7th March 2006 and brought into operation with effect from 1st October 2007 (vide *Gazette Extraordinary No. 1516/25 of 27th September 2007*). The Act was prepared consequent to a decision of the Cabinet of Ministers, dated 22nd October 2004, directing that legislation on Electronic Transactions be prepared with legal and policy inputs from the ICT Agency of Sri Lanka (ICTA). This process was initiated through a "*Joint Cabinet Memorandum*" of the Prime Minister, the Minister of Trade and Commerce, the Minister of Science and Technology, with support from the Ministry of Finance.

As a follow-up to the enactment of the Electronic Transactions Act, Sri Lanka became the first country in South Asia (and one of the first three countries in the Asian Region) to sign the *United Nations Convention on the Use of Electronic Communications in International Contracts* (commonly known as the e-Contracting convention). This was consequent to a Cabinet decision initiated jointly by the Ministry of Science and Technology and Ministry of Foreign Affairs.

2.1 General Features of the Electronic Transactions Act

The Electronic Transactions Act 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). Therefore, the language, key words and definitions used in the Act are consistent with the aforesaid international legal instruments.

The preamble to the Legislation states that it is "*AN ACT TO RECOGNIZE AND FACILITATE THE FORMATION OF CONTRACTS, THE CREATION AND EXCHANGE OF DATA MESSAGES, ELECTRONIC DOCUMENTS, ELECTRONIC RECORDS AND OTHER COMMUNICATIONS IN ELECTRONIC FORM, IN SRI LANKA; AND TO PROVIDE FOR THE APPOINTMENT OF A CERTIFICATION AUTHORITY AND ACCREDITATION OF CERTIFICATION SERVICE PROVIDERS; AND TO PROVIDE FOR MATTERS CONNECTED THEREWITH OR INCIDENTAL THERETO*"

The objectives **of the Act, as stated in Section 2, are as follows:-**

(a) to facilitate domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty;
(b) to encourage the use of ***reliable forms of electronic commerce***;
(c) 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
(d) to promote public confidence in the authenticity, integrity and reliability of data messages and electronic communications. (*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.

Three fundamental policy principles form the basis of the Sri Lankan Electronic Transactions Act. They are (a) *technology neutrality*, (b) functional equivalence and (c) party autonomy (*emphasis added)*.

Technology Neutrality is ensured in the Electronic Transactions Act by not dictating the technology which would be given legal preference[3]. For instance the definition and description of "**electronic signature**" in Section 26 ensures that the *authenticating technology* solution for use of *Electronic Signatures*, as envisaged under Section 7, should be "....incorporated in or logically associated with an electronic document, with the *intention* of authenticating and/ or *approving* the same...."[4]. The Act does not specify any technology which should be used.

2.2 Other Features of the Electronic Transactions Act

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.

---

[3] Section 7 of the Electronic Transactions Act. See also the definition of "Electronic Signature" in Section 26 of the Act

[4] Vide definition of "Electronic Signature" in Section 26 of the Act

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.

2.3 Establishment of Certificate Authority and CSPs

At the outset it should be noted that amongst the stated objectives stipulated in Section 2 of the Act. provides for the use of authentication technologies (eg:- electronic signatures) for secure transactions in Sri Lanka [see Section 2(b), (c) and (d)]. "*Technology neutral*" nature of the Electronic Transactions Act is an important policy consideration in the establishment of a Certification Authority[5] and Certification Service Providers (or operational sector specific CAs'[6]), within the framework of the Act.

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.[7]

---

[7] Section 18(1)of the Electronic Transactions Act,

[5] This could take the form of a "Root CA" or a" National CA" (depending on the functions carried out)

[6] Sector specific CA's such as LGN CA and Lanka Clear CA would be CSPs' under the Act

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.

At the time the Act was brought into operation the provisions of Section 18 and 19 were specifically left out in the *Gazette Extraordinary No. 1516/25 of 27th September 2007*. At the time there was NO unanimity in the identification of an entity to perform the function of a "root" or "national" CA, though there was some consensus that the functions of this entity should be administered by ICT Agency (ICTA). But no order has so far been made to designate a CA. The **underlying intention of excluding Section 18 and 19** from operation seems to indicate Government's intention of not subjecting the CSPs' or operational / sector specific CAs' with additional regulatory or administrative burdens.

It is important to emphasise that in designating a CA under Section 18, the Minister is required by Law to consider the overall ability of the Government Department or other Institution to be designated as the CA "to discharge the obligations under this Act in ensuring the proper functioning of certification services by *accredited* Certification Service Providers (CSPs)."[8] It is significant that the Electronic Transaction Act of Sri Lanka differs from similar legislation enacted in India[9] and elsewhere in one important respect. While in many countries CSPs are required to be licenced to engage in the business of providing certification services, the Sri Lankan legislation does not mandatorily require or insist on a licence. The *accreditation* provided in the Act is also optional.

Although Section 20(1) of the Act provides that "no person shall function as an Accredited Certification Service Provider (ACSP) unless he holds a valid Certificate of Accreditation[10], issued under the Sri Lanka Accreditation Board for Conformity Assessment Act of 2005[11]," Section 20(2) expressly states that "*nothing in this Act shall be construed as impeding or in any way restricting the rights of any certification service provider to engage in the business of providing certification services* ***without*** *being accredited*."

The Certification Authority (CA) designated under Section 18 has the power to identify the criteria which will form the basis for accreditation of CSPs', the qualifications required by them and is also empowered to specify the procedure to be followed in granting of accreditations and

---

[8] See Section18(2)

[9] Sections 21-26 of the Indian Information Technology Act, 2000 provide for the procedure for licensing of service providers in India, and Section 19 provides for the recognition of foreign certifying authorities. The Act contains elaborate provisions for investigations of contraventions of the Act and also sanctions stringent penalties

[10] Section 20(3) of the Sri Lankan Electronic Transactions Act, provides for the issue of a Certificate of Accreditation in terms of the Sri Lanka Accreditation Board for Conformity Assessment Act No. 32 of 2005 to CSPs in accordance with the provisions of the latter Act "in keeping with the criteria for accreditation specified by the Certification Authority...."

[11] The Sri Lanka Accreditation Board for Conformity Assessment Act, No. 32 of 2005

hearing of appeals in the event of a refusal to grant or renew accreditation under Section 20 (Vide Section 19). It is also relevant to note that the Certification Authority (CA) designated under Section 18 has the power to "*issue licences or any other form of authorisation* to CSPs to provide *prescribed services*". This is **independent** of the powers relating to accreditation outlined above and seems to suggest that licenses could be issued to CSPs' to provide sector specific services (eg:- for Lanka Clear Ltd or Lanka Govt Network) or other designated services or even special services through special licenses, over and above the general business of providing certification services. The relevant Minister is specially empowered by the Act to specify by regulation, the procedure for the recognition of CSPs, the issue of licences to such providers and the categories of services required to be provided by them.[12]

As such, **there could be three kinds of CSPs under the Act**, namely Licensed Certification Service Providers (LCSPs) to provide "*prescribed services*", Accredited Certification Service Providers (ACSPs) and ordinary Certification Service Providers (CSPs) providing certification services without any licence or accreditation. With respect to all categories of CSPs, irrespective of whether they are licensed or accredited, the Certification Authority (CA) has the power to require that they maintain such records and registers as may be prescribed and to call for information as may be necessary from time to time and issue directions. Section 18 and 19 NOT being in operation do not preclude or prevent a CSP established by a government or private entity from commencing operations, as provided for in Section 20(2) of the Act.

2.4 Establishment of Certification Services in the Banking & Government Sector

Consequent to the enactment of the Electronic Transactions, two Certification Service Providers have established operations in Sri Lanka.

In May 2009, Lanka Clear Ltd, the Company owned jointly by the Central of Sri Lanka together with all licensed Commercial banks, which has also been statutorily empowered under Section 98 of the Monetary Law to handle all interbank payments, launched the ***Sri Lanka's first Certification Service Provider***. This effectively became the first Financial sector Certificate Authority issuing Digital Certificates to commercial bank. This service became known as ***Lanka SIGN***.

The Payment and Settlement Systems Act No. 28 of 2005 provides the framework for the deployment of innovative technologies to enhance banking operations. In March 2006 Sri Lanka became the first in South Asia to implement a nationwide Cheque imaging and Truncation System (CITS) and it is envisaged that a Common payment Switch would be operational at some point to support online real-time fund transfers and payments between commercial banks.

With these systems coming into operation, the deployment of Lanka SIGN becomes all the more significant. The use of digital certificates issued to Licensed Banks by Lanka Clear, in the Cheque Imaging & Truncation system, would ensure greater authenticity, integrity and reliability to the transaction and the said transactions could benefit from the provisions of the Electronic

[12] *See,* Section 24(2)(g) of the Electronic Transactions Act

Transactions Act of 2006, especially the rules governing evidence. The Launch of Lanka Sign as the first Certification Services Provider has set the framework for the establishment of other similar services in Sri Lanka and would lead to the creation of the National level Certification Authority under the Electronic Transactions Act.

In November 2009 the 2nd Certification Services Provider was established under the auspices of ICT Agency of Sri Lanka (ICTA). This became known as the "***Lanka Government Network – Certificate Authority***" (LGN-CA). The LGN CA is designed to facilitate the digital certificate requirements of the public sector Government organizations in Sri Lanka. LGN-CA will issue digital certificates to organizations after following a specified request validation and approval procedure. A digital certificate issued by LGN-CA can be used in many software applications to provide confidentiality through encryption, authenticity and non-repudiation through digital signatures, identification and authorization through authentication protocols, as well as shared secret key distribution for secure session management, etc. Transactions on the Lanka Government Network (LGN) can use these security services to ensure privacy of users on LGN, protect the data being transmitted and ensure that transactions are in compliance with Electronic Transactions Act as well as the Computer Crimes Act.

The public key infrastructure (PKI) capabilities provided by LGN-CA, including digital certificate issuance, renewal, revocation and status verification can be used to implement access control policies to resources hosted on the LGN. The LGN-CA operating model is based on providing different types of digital certificate classes to match different Government organizational security policy levels.

Both LGN-CA as well as Lanka SIGN (established by Lanka Clear) would take the form of an ordinary Certification Service Providers (CSPs) or sector specific CAs, providing certification services without any licence or accreditation. When Section 18 and 19 of the Electronic Transactions Act are brought into operation and an appropriate "national" entity is identified as a Certification Authority, such national entity could perform the functions of a "Root CA". There is no reason to have another separate body. The technical functions of a "root" CA may be outsourced to the national entity.

The "Sector specific CAs'" or "CSPs" (ie Lanka SIGN and LGN-CA) which have already commenced operations, before Section 18 and 19 were brought into operation, may subject themselves to either a "License" or "Accreditation" under the Electronic Transactions Act. As explained earlier this is ***optional*** and not mandatory.

2.5 Electronic Evidence Regime – The Problem

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[13] 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".[14] The Ordinance also declares that "primary evidence means the document itself produced for the inspection of the court"[15]. 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",[16] 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*[17] 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 Ordinance[18] 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 case[19], 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:-

[13] Evidence Ordinance of Ceylon No. 14 of 1895(CLE 1956 Official Ed. Cap. 14) as subsequently amended

[14] § 64 of the Evidence Ordinance of Ceylon

[15] § 62 of the Evidence Ordinance of Ceylon

[16] Peiris G.L, *The Law of Evidence in Sri Lanka,* p.42. For an interesting illustration of the application of the rule see,

D.Somasiri v The Queen 75 New Law Report of Sri Lanka (NLR), 172

[17] [1978-79] 2 Sri L.R. 194

[18] Identical provisions are found in the Indian Evidence Act of 1872 as well

[19] *Robin vs Grogan*, Per Howard CJ, (1942) 43 NLR 269, 270

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.[20]

2.6 Electronic Evidence Regime – The Solution

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 4 of the Evidence (Special Provisions) Act No.14 of 1995 provide for the admissibility of information contained in contemporaneous recordings, Section 5 of the said Act provides for the admissibility of Information Produced by Computers ("Computer Evidence"). It is important to note that the provisions of the Special Provisions Act are applicable to both criminal and civil proceedings.

Two sets of conditions become applicable under the Evidence (Special Provisions) Act depending on the inherent credibility of the process, which forms the basis of the information sought to be produced.

(1) A liberal regime is provided for the admissibility of information produced in the course of any regularly conducted activity;
(2) A more stringent regime when such information is produced outside such activity (mostly information produced for a specific purpose).

The justification for such a distinction is the recognition that any restrictions in the form of conditions to admissibility must be varied and should correspond to the level of credibility that could be attached to the evidence (i.e. information produced by computers) sought to be admitted.

In this respect information produced in the course of any business or regularly conducted activities is treated as having far greater credibility than information produced for a specific purpose, mostly after the event on in the anticipation of an event that could lead to the necessity of legal proof.

Following closely on some of the approaches adopted in the Evidence (Special Provisions) Act, is the Electronic Transactions Act No. 19 of 2006, which tends to expand the modalities through which electronic evidence could be admitted. This is also achieved through conditions which are far more flexible than the provisions contained in the Act No. 14 of 1995.

[20] E R S R Coomaraswamy, *The Law of Evidence*, Vol II , Pg 105-106

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,[21]

shall be admissible in any proceedings."[22]

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"*.[23] The ***third*** presumption is to the effect that a court will presume the genuineness of any electronic signature unless the contrary is proved.[24]

---

[21] This provision is based on the fundamentals of the Business Records Exception to the hearsay rule contained in Evidence
Ordinance of Ceylon No. 14 of 1895 (CLE 1956 Official Ed. Cap. 14)

[22] § 21(2) of the Electronic Transactions Act

[23] § 21(3) of the Act

[24] *Ibid.*

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.[1] 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.

3. Dealing with Technology Abuses – Computer Crimes Act of 2007

Sri Lanka responded to the Cyber Security challenge by enacting the Computer Crimes Bill on 8th of May 2007. This Bill, which was certified by the Speaker of Parliament on 9th July 2007, as **Computer Crimes Act No. 24 of 2007,** was brought into operation with effect from 15th July 2008. This legislation is the result of joint contributions from CINTEC Committee on Law & Computers[25] (1995-2000), Computer Crimes Sub-Committee of the Law Commission and the Ministry of Justice (2001-2004) and ICT Agency of Sri Lanka (2004 – 2007).

During the early stages of the Drafting process the provisions contained in the Penal Code of Ceylon - 1885 (with emphasis on Offences against property) were examined in order to determine whether the Penal Code could be modified and adapted to deal with Computer Crime related offences. However, it was felt that definitions of offences such as THEFT, Cheating and Criminal Misappropriation (and the definition of property) in the Penal Code of Ceylon were limited in scope and basically reflect the conditions that prevailed in the previous century. It was found that those definitions were formulated on the assumption that an identifiable human offender and victim are in existence and envisaged the commission of an act in a specified manner by the offender against the victim. As such it was decided to pursue a *sui generis* approach to legislation.

[25] 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)

During the formulation of the legislation in Sri Lanka it was agreed that the term "Computer Crime" is a generic term used to identify all crimes or frauds that are connected with or related to computers and information technology. As such the term "computer crime" is not defined in the Act and legislators felt that it was synonymous with "Cyber Crime", although the latter tends to be focussed towards criminal activity resulting from the use of the internet.

3.1 Computer Crimes Act – Key provisions

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[26].

[26] Illustrations to Section 5 of the Sri Lankan Computer Crimes Act identifies broad categories of offences which constitute 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[27], 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[28] 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 was 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[29].

3.2 Investigation and Enforcement

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.

[27] Also known as the Budapest Convention (2001)

[28] New Sections 286B and 286C introduced through Penal Code (Amendment) Act No. 16 of 2006

[29] The term "Payment Devices" covers a wide range of instruments, including a credit card or device containing account number or other information relevant to the holder of such device etc (See Section 32 of the Act)

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[30].

These designated experts are fully empowered and given protection under the legislation[31]. 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[32]. 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.

3.3 Challenges

Despite the aforesaid safeguards, the challenge is to get the required regulations designating the said experts or even to get experts to volunteer to be so designated to support the investigative process. A common concern expressed by experts is whether they would be called upon to give evidence, thus exposing them to cross examination in a court of law. As such many capable experts have shown reluctance to be designated under the Computer Crimes Act[33]. The procedural laws have not yet been amended to facilitate the submission of affidavit evidence on matters concerning sensitive investigations.

---

[30] Section 17 of the Computer Crimes Act No. 24 of 2007 & Section 8 of the Payment Devices Frauds Act No. 30 of 2006

[31] Section 18 and 28 of the Computer Crimes Act (See also Part II of the Payment Devices Frauds Act)

[32] See for instance Section 20 of the Computer Crimes Act (ordinary course of legitimate business not to be hampered in the course of investigations); and Section 24 (ensuring confidentiality of information obtained in the course of an investigation)

[33] Regulations have been promulgated designating "experts" under the Payment Devices Frauds Act No. 30 of 2006 – See Payment Devices Frauds Regulations, No. 01 of 2008 made by HE the President, published in Gazette Extraordinary of 14th February 2008

The second challenge is to ensure the admissibility of electronic or computer based evidence. Although the existing evidence laws permit the admissibility of Computer generated records[34], admissibility is subject to several stringent criteria[35], as discussed in Para 2.6 above.

It is left to judicial interpretation to determine to what extent the more flexible rules governing Evidence contained in the Electronic Transactions Act 19 of 2006 would be applicable to proceedings under the Computer Crimes Act. The Computer Crimes Act is silent on the matter and does not contain a specific admissibility regime. If any Computer Crime arises out of an electronic based transaction, it may be possible to invoke the provisions in the Electronic Transactions Act, only to admit the information contained in a data message, electronic record etc, within the presumptions contained in Section 21(3) of the said Act (as discussed in Para 2.6 above), although the provisions contained therein may be construed to be admissible only in civil or commercial cases, in view of the deviation from the hearsay rule as provided for in Section 21(3) of the Act. This is an area requiring review and consideration and further legal reform.

3.4 Institutional Measures – Sri Lanka CERT

Many Governments are increasingly relying on a broad range of resources outside the traditional Governmental law enforcement expertise to address Cyber threats and forensic issues. As such new institutional models may have to be created. The Sri Lankan experience is an interesting example.

In mid 2006 Sri Lanka CERT[36](Computer Emergency Response Team) was created to address cyber security incidents. This is a government owned company (a subsidiary of ICT Agency of Sri Lanka- ICTA)[37], established with support from World Bank, and runs on a private sector driven model with highly skilled incident handlers. The Board consists of a range of key stake holders such as enforcement authorities, bankers, Private sector and academia.

SLCERT was admitted as a full member of APCERT and became the first South Asian CERT to be admitted as a full member of FIRST[38] in 2008. In just a few years SLCERT has responded effectively to the Cyber Crime forensic issues. Due to the requests from law enforcement agencies SLCERT started offering digital forensics as a service for law enforcement agencies since the third quarter of 2008. SLCERT also carries out forensic investigations for other government establishments in Sri Lanka.

---

[34] Evidence (Special Provisions) Act 14 of 1995
[35] Eg – Certificate that the computer was working properly etc
[36] www.slcert.gov.lk
[37] www.icta.lk
[38] www.FIRST.org

4. DATA PROTECTION

This subject has become important in an era where information systems are used by the banking and financial sector to collect, store and process personal information. Data protection laws have been present in Western Europe for some 35 years. Such legislation originated in European human rights law, specifically the right to privacy enshrined in article 8 of the European Convention on Human Rights. However, data protection laws do not map neatly onto a privacy framework, but rather represent a range of differing interests. A broad distinction can be made between 'interests that relate to the quality of (personal) information and information systems', such as accessibility and reliability, and 'interests pertaining to the condition of persons as data subjects and to the quality of society generally', such as privacy, autonomy and democracy[39].

As a consequence of this broad range of interests, data protection laws should not be seen as simply a subset of privacy law, but rather a distinct but overlapping topic, which also addresses data quality and data security issues.

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.

4.1 Policy Issues and Regulatory Approach

Prior to examining the content and structure of a data protection regime, it is worth briefly reviewing some of the policy concerns that drive a regulatory response in the area of data protection, since the regulatory product will generally reflect the nature of these concerns. In terms of policy drivers, the demand for a data protection regime may primarily originate from a domestic agenda or from developments abroad.

At a domestic level, data protection will generally be focused more towards concerns about the use and abuse of personal data by the public sector, rather than the private sector. This is the case in Thailand, for example, under the Official Information Act[40]; while the Commonwealth Model Privacy Law also only addresses public sector uses and abuses of personal data. The value of an individual's data is obviously directly related to a nation's state of economic development, the sophistication of private sector activity, and the purchasing power of consumers.

Personal data as an asset is a particular feature of service sector economies, specifically the Information economy, not agrarian or industrialising economies. The interest of citizens, protected

[39] See Bygrave, L., *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer, 2002.
[40] See http://www.oic.thaigov.go.th/

from arbitrary government interference and participating in the democratic process, generally drives data protection regulation.

Alternatively, the pressure for a regulatory response to protect personal data may arise from developments abroad. Sri Lanka perceives a need to address issues of data protection to facilitate their participation in the expanding global information economy, and to ensure that the absence of protection does not constitute a non-tariff trade barrier to the flows of data from developed nation economies.

India, for example, has been extremely successful in developing an outsourcing industry, from basic data entry processing to customer call centres, based on a literate work force and a developed computer and communications infrastructure[41]. Indian businesses have attracted a wide range of Western companies, from financial services to utilities, to relocate various business processes to the sub-continent. The same trend is found even in Sri Lanka. However, concerns have been voiced in the European Parliament about the vulnerability of personal data being transferred under such outsourcing arrangements[42]. Some view outsourcing as a process that effectively circumvents European regulatory safeguards.

Whether calls for data protection regulation reflects domestic concerns or is reactive to the legal situation in other countries, consideration obviously needs to be given to the most appropriate regulatory approach. The approaches taken by jurisdictions to implement the data protection principles (see below) have generally developed along three different but overlapping lines:

- The *comprehensive regulatory approach* requires the creation of a general law laying down rules for the collection, use, and dissemination of personal data in both the public and private sectors, enforced by a supervisory authority or regulator.

- The *sectoral approach* relies on localised legislation, where there is a clear threat and high risk of harm if personal data are misused, such as the financial sector or in the case of data relating to health or to children. There is no national oversight agency.

- The *co- or self-regulatory approach* can be considered a hybrid of the comprehensive and sectoral approaches. A minimum level of protection is adopted, with or without a statutory footing[43], with different sectors implementing codes of practice that apply the protections to the practices in each sector. Supervision may be carried out by an industry body, although with some independent or public authority oversight.

Any conflict between these approaches is centred around methodology and scope, and not on the underlying principles of protection.

[41] See Chapter 5 on 'Business Process Outsourcing Services for Economic Development', pp.135-152, in UNCTAD *E-Commerce and Development Report*, 2003.

[42] E.g. 'EU targets offshore data', *IT Week*, 13 April 2004.

[43] The presence or absence of a formal legal basis represents the key distinction between co- and self-regulation.

4.2 The Data Protection Approach for Sri Lanka ?

Given the upsurge of BPO related investments in Sri Lanka, ICTA has been compelled to take a decision to pursue 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 No. 27 of 2003. As such, this approach can be seen as self- or co-regulatory.

For a country such as Sri Lanka, the cost of regulation will obviously be a critical factor. The cost associated with a comprehensive or omnibus approach, specifically the establishment of a dedicated regulatory authority, will generally be excessive for most developing countries, especially if borne by the private sector through licensing or notification fees. A sectoral regulatory response may be appropriate to address specific uses and abuses of personal data, whether driven by domestic or foreign concerns.

Whilst a self-regulatory or co-regulatory approach may be appealing in terms of minimising the public costs of regulation, its success depends, first and foremost, on a sufficiently strong and active private sector, willing and able to fund the regulatory supervision and, second, a court system capable of dealing with allegations of damage caused by breaches of the data protection rules. It seems that the financial sector as well as the BPO sector has reached sufficient maturity in this connection.

Codes of practice are given explicit recognition under the EU General Directive as a mechanism for contributing to the proper implementation of the national provisions (art. 27). In this context, therefore, such codes are viewed as supplementary rather than stand-alone. Various codes have been drawn up at a Member State and Community level by trade associations and other industry bodies in Europe, such as the Federation of European Direct and Interactive Marketing (FEDMA) 'Code of Practice for the Use of Personal Data in Direct Marketing'[44].

Non-European jurisdictions have also recognised the use of codes as a key element in a data protection framework. In New Zealand, Australia and Hong Kong, for example, codes are given legal recognition and, in some cases, legal force[45]. In the first two jurisdictions, the adoption of a code supersedes the principles detailed in the legislation. However, these codes are generally organisational or industry sector-based, rather than generically applicable across the private sector. The two leading examples of such generic codes, and therefore of key relevance to Sri Lanka's deliberations, are the US 'Safe Harbor' agreement and the Singapore Model Code.

---

[44] http://www.fedma.org/img/db/FEDMACodeEN.pdf

[45] I.e. the New Zealand Privacy Act 1993, the Australian Privacy Amendment (Private Sector) Act 2000 and the Hong Kong Personal Data (Privacy) Ordinance 1995.

5. Legislative reforms to facilitate e-Transaction in the Banking sector

In terms of Section 113 of the Monetary Law Act, Central Bank of Sri Lanka (CBSL) as the fiscal agent of the Government, is responsible for the management of Public Debt. The Public Debt Department (PDD) of the CBSL is engaged in activities relating to the issuance, servicing and management of domestic debt and servicing of foreign debt on behalf of the Government. Domestic debt is confined mainly to instruments such as Rupee Loans, Treasury Bonds and Treasury Bills.

The Rupee Loans and Treasury Bonds are issued under the provisions of Registered Stock and Securities Ordinance (RSSO) whilst Treasury Bills are issued under the provisions of Local Treasury Bills Ordinance (LTBO). The issue of instruments provided in the Treasury Certificates of the Deposits Act (TCDA) and Tax Reserve Certificates Act (TRCA) would also result in public debt. However, such debt instruments have not been issued in the recent past. The issue of foreign loans comes under the purview of Foreign Loans Act

The government securities have been hitherto issued in the form of scrip (paper) securities. With the introduction of Scripless Securities Settlement System (SSSS), initially Treasury Bills and Treasury Bonds will be issued in scripless form. The SSSS is based on a computer network where trading and ownership of government securities are recorded on an electronic platform. In the SSSS, licensed commercial banks who have been appointed as Dealer Direct Participants will hold accounts on their behalf and on behalf of other investors who will be their customers. Any other institution permitted by the Central Bank as a direct participant will hold accounts on their own behalf only. Investor risks associated with holding and trading of paper based securities will be totally eliminated under the SSSS. The investor will not be subject to the hassle of dealing with physical certificates of government securities hitherto experienced. The new system will operate on Delivery Vs Payment (DVP) basis.

The scripless securities will improve efficiency in the government debt securities market. With the introduction of the SSSS, the need for physical delivery and verification of certificates will not arise. Therefore, the introduction of the SSSS will reduce human intervention and the need for physical verification of securities thus resulting in the enhancement of efficiency. The scripless securities will eliminate the risks associated with paper based securities. Risks involved in physical movement of scrips will be reduced to zero in CDS which will maintain all records electronically.

The paperless (scripless) trading was made possible through the Monetary Law (Amendment) Act of 2002, as well as the Local Treasury Bills (amendment) Act No. 1 of 2004 and Registered Stocks and Securities (amendment) Act No. 2 of 2004.

LankaSecure and entity established by the Central Bank is the registry as well as the custodian for government securities. The payments on settlement of scripless securities transactions are based on a Real Time Gross Settlement System (RTGS) where funds are transferred electronically.

Another entity known as Lanka Clear, under the Central Bank, is engaged in the facilitation of Cheque imaging under Payment and Settlement Systems Act No. 28 of 2005.

5.1 Legal Framework for Scripless Securities Trading

The establishment of a central depository (CDS) and a settlement system for transactions on electronic basis were made possible by the Monetary Law Act as amended by Act No.32 of 2002. This amendment allows the Central Bank to function as a Certification Authority for the purpose of issue e-signature certificates to participating banks.

The Local Treasury Bills Ordinance (Amendment) Act No. 1 of 2004 and the Registered Stock and Securities Ordinance (Amendment) Act No. 2 of 2004 provide for converting existing Treasury Bills and Treasury Bonds which had been issued in scrip form into scripless form. The system rules, regulations and guidelines issued to the participants in terms of the above legislations will facilitate the operations described above.

These legal reforms have facilitated the introduction of a unique system bond and securities trading system in Sri Lanka by the Central, the **first of its kind** in South Asia.

6. Conclusions

The effective adoption of the Scripless Securities Trading System as well as the implementation of the Cheque Imaging and Truncation System (CITS) demonstrates the ability of the Banking & Financial sector in Sri Lanka to be e-ready to transform itself to the next stage. The financial sector in Sri Lanka has been at the forefront of technology adoption, manifested by the first sector specific certificate authority being established by LankaClear. Technology innovations adopted by the banking sector has even helped government of Sri Lanka to provide services via the internet as seen in the e-revenue license system facilitated through LankaGate (www.srilanka.lk). However with increased use of technology comes several vulnerabilities, which have been effectively dealt with through legislation as explained above.

From the analysis contained in this article, it would be apparent to our stake holders that the legal system in Sri Lanka has kept pace with the developments in technology by providing the framework for electronic based activity to reach a level of maturity commensurate with the rest of the emerging world. Some of the recent enactments referred to above and other proposed changes are only an initial step in achieving the objective of transforming our nation into an e-Enabled framework. The Government together with the private sector remain committed to drive the reform efforts to help Sri Lanka become another "financial hub" of Asia. The legislative framework has been strengthened by the recent adoption of an e-Government Policy[46], which creates greater certainty when transacting with Government agencies via electronic means.

[46] Policy and Procedures for ICT usage in Government (eGovernment Policy), adopted by Cabinet of Ministers on 16th December 2009 and conveyed to all Government Organisations through Circular of Secretary to President, dated 31st May 2010.