

IMPACT OF RECENT IT RELATED LEGISLATION

Jayantha Fernando¹

1.0 INTRODUCTION

This article outlines some the recent developments in relation to IT & Law. The focus would be on provisions governing Software and Intellectual Property Rights, with reference to the Intellectual Property Act No. 36 of 2003, Electronic Transactions with reference to Act No. 19 of 2006, Computer Crimes, Data Protection and some of the recent related legislation.

2.0 Intellectual Property Rights – Copyright and Software Protection

Copyright protection has traditionally been viewed as offering an incentive for the production of artistic, scientific, and other creative content, while permitting the public to access, use and innovate with such creative works.

The Internet and other global information technologies have opened new opportunities for the creation, distribution, and use of creative content. The Internet challenges lawmakers and society as a whole: how to preserve the balance between creators' rights and users' rights? Can the foundations of copyright law withstand the pressures of the new technologies? Can they be interpreted to apply to the modern age?

The purpose of this note is to clarify some of these issues

2.1 Copyright measures to protect Software in Sri Lanka

An important aspect of legal reform which has been successfully implemented in Sri Lanka is the Intellectual Property measures to ensure adequate and meaningful protection for Computer Software. Over the years, Copyright as a means of protecting Software under the Intellectual Property regime became accepted firstly through judicial dicta² and then through statute law³ and International legal covenants⁴.

Traditionally, in almost all commonwealth jurisdictions, Computer Software whether it be programs, databases, Computer files, preparatory design materiel and all associated printed documentation are all protected under the Copyright regime. This was re-asserted in Sri Lanka when the principles contained in the Amendment Act No 40 of 2000 were re-introduced through the Code of Intellectual Property Act No. 36 of 2003.

Consequent to the Amending Act No. 40 of 2000 the first Source Code IP infringement case was filed before the Commercial High Court of Colombo (*Soft Systems Pvt Ltd vs Visual Tech Ltd*). Although the Court granted enjoining order in the case, the action was dismissed for want of appearance during the Injunction Inquiry.

¹ LLM – ICT & Telecom Law (Lond), *Attorney-at-Law*, Legal Advisor, ICT Agency of Sri Lanka (ICTA)

² Eg:- *Apple Computer Inc vs Computer Edge Pty Ltd* [1984] FSR 481

³ Intellectual Property (Amendment) Act No. 40 of 2000 – amending the provisions of IP Code of 1979

⁴ Eg:- Australian Copyright Amendment Act (1984), UK Copyright (Computer Software) Amendment Act (1985) and the 1994 WTO TRIPS Agreement

2.2 Copyright Software protection under the code of Intellectual Property Act No. 36 of 2003

Under Section 6(1)(b) of the new IP Act No. 36 of 2003, Computer Programs are protected under the Copyright regime within the scope of literary, scientific and artistic works (as in the Amendment of 2000). Similarly, the words “*Computer*” and “*Computer Program*” have been defined in accordance with the WIPO Model Provisions for the protection of Computer Software complying with Article 10(1) of TRIPS. What is required under Section 6 to protect Software is to satisfy the test of originality. Most Software programs would meet the requirement of originality, even if the program comprises little more than an arrangement of commonly used sub-routines, because even the selection and arrangement of such sub-routines require a reasonable amount of skill and expertise (sometimes referred to as the test of “skill, labour and judgement”)⁵.

In terms of Section 9 of the IP Code 2003 the *owner* of a Copyright protected work “shall have the *exclusive right* to carry out or to authorize (a) the reproduction of the work (b) to translate the work (c) Carryout adaptations to the work etc. From a Software perspective this would mean that acts, such as the conversion of Software Source Code to Object Code format and even reverse engineering of Software would have to be exclusively carried out by the lawful owner.

A new feature in relation to Software protection under the IP Code of 2003 is the inclusion of a provision governing “fair use” in relation to Software. The concept of “fair-use” is an exception to the general rules governing Copyright protection. Section 12(7) of the IP Code provides that a reproduction in a single copy or the adaptation of the Computer program by the lawful owner of a copy of that Program (eg:- by the Licensee), shall be permitted without authorization of the owner of the Copyright if the copy or adaptation is required (a) for the purposes and the extent for which it was originally obtained, and (b) for archival or replacement of the lawfully owned copy of the Computer Program in the event the said copy is lost, destroyed or rendered unusable.

2.3 Software Copyright protection and Open Source licensing

Open Source Software which is increasingly becoming popular even amongst individual users is being made available under a variety of licensing approaches. They all have a common feature, i.e. rely on Copyright to form the licensing contract. There are two principle open source licensing approaches – the GNU General Public License (GPL) and the Berkeley Software Distribution (BSD) License. Under the GPL, all derivative works must be licensed on the same terms as the original Software and source code subject to GPL cannot be disassociated with that license. Under BSD, developers are allowed to integrate the licensed software with developers’ own source code to create new products with few restrictions. Therefore, programs containing BSD code do not have to be re-distributed under the BSD license terms and instead could be subject to separate license terms.

The basis on which Open Source License categories impose terms and conditions on the use of the code is also founded on elements of Intellectual Property rights, namely, the copyright regime. In terms of most license conditions imposed under Open Source Models, the use of Source Code is permitted on condition that there is an appropriate attribution to the author of the original source code.

⁵ *Cramp & Sons Ltd vs Frank Smythson Ltd* [1944] AC 329; *Feist Publications vs Rural Telephone Services* (1991) 111 S Ct 1282

In a recent German case ⁶, a three judge German Court gave recognition to the GPL by requiring the defendant company to disclose the Source Code of its product that contained components of Open Source Software. The Plaintiff's case was founded on Copyright. This illustrates that both in Open Source and commercial software models, the Copyright IP model remains the foundation for the license conditions.

2.4 The “idea-expression dichotomy”

The safeguards provided in the IP Act of 2003, mentioned above, contain adequate safeguards against literal copying of Software. This means that sufficient protection is given to situations where exact duplicates are made through disk-to-disk copying.

In several jurisdictions, the basis for safeguarding Software from non-literal copying is increasingly becoming more and more uncertain. This is in view of the fact that copyright per-se does not give a monopoly over the ideas; what it does is to prevent a person from copying or otherwise using the tangible expression of ideas of the Copyright holder. In other words Copyright only protects the expression of ideas and not the idea itself.

Copying from a Software perspective can take a variety of forms. It need not be limited to taking a disk-to-disk duplicate. It is possible to copy a Computer program in a wider sense, for example the structure, flow and sequence of operations expressed in a Computer program may be copied and if a different programming language is used, the print out of the source code of the second program may NOT look similar to the first program.

In *Whelan Associates vs Jaslow Dental Laboratories Inc.*,⁷ the impugned program was designed to assist dental labs. The same person was involved in the development of the competing programs but both were written in different computing languages. The first was written in EDL and the second (intended for the microcomputer market) written in BASIC. Therefore, there was no substantial literal similarity between the listings of the two programs. The US Court of Appeal (3rd Circuit) distinguished between the idea and expression and held that the purpose sought to be achieved, namely, the running of dental labs was the *idea*, which was not protected by Copyright and stated that it was quite acceptable for others to write similar programs in different languages. However, in this instance the structure of both programs was the same and so did the look and feel and because both were done by the same person, it was held that there was a possibility of a copyright infringement.

In *Lotus Development Corp vs Borland International Inc.*,⁸ Lotus claimed that the defendant (Borland) had copied the same menu system for a competitive spread sheet program. Both products were electronic spreadsheets intended to facilitate accounting and other processes that involve the manipulation of and display of numerical data. It was held that the menu command hierarchy in the Lotus 1-2-3 spread sheet was an idea and therefore not copyrightable.

Even in UK the trend has been similar⁹. Therefore, if a company develops a unique piece of Software which proves to have extensive marketing success, then, another company could develop their own version in order to gain a share of the market (based on the first program). Copyright Law does not prevent this as long as the first program is not literally copied (i.e subject

⁶ Netfilter Project VS Sitecom Germany GmbH (2004)

⁷ 1987 FSR 1

⁸ [1997] FSR 61

⁹ eg:- Cantor Fitzgerald vs Tradition (1999) & IBCOS Computers vs Barclays Mercantile Ltd [1994] FSR 275

to disk to disk copying) or adapted. This principle in a way has been established in the EU Software Directive¹⁰. Article 1(2) of the said Directive explicitly requires all EU member countries to protect Computer Programs as literary works but to exclude from protection “ideas and principles which underlie any element of a computer program, including those which underlie its interfaces”.

2.5 Additional protection measures for Software

A new feature of the IP Act No. 36 of 2003 is the inclusion of a specific provision granting adequate protection to “undisclosed information”. This is consistent with Article 39 of the TRIPS Agreement. Section 160(6) of the Act provides that the disclosure and acquisition of undisclosed information without the consent of the “the rightful holder” would constitute an act of unfair competition. Section 160 (6)(b) further elaborates the above stating that the disclosure, acquisition or use of undisclosed information by others without the consent of the rightful holder may result from (a) industrial espionage (b) Breach of contract (c) Breach of confidence etc.

Therefore, these provisions in the IP Act of 2003 in effect gives statutory recognition to the English common law principles under the Law of confidence, providing sufficient safeguards to all aspects information, including the ideas behind the software¹¹ and information relating to preparation of Software. The requirement is to have proper contractual arrangements between the owner of such information and the user. The use of Non-disclosure Agreements (NDA) accompanying contracts of employment has become a phenomena in the Software industry even in Sri Lanka. In the context of the above provisions the breach of such contractual obligations would attract the provisions of Section 160(6) (b) of the IP Act of 2003 and may constitute an act of unfair competition.

Even prior to the enactment of the IP Act of 2003 confidential information was protected by means of contract law through appropriate contractual measures such as Non-disclosure agreements. In *Precision Tech Services (Pvt) Ltd vs Ingram Micro Asia Ltd*,¹² the Commercial High Court of Colombo recognized in principle the concepts embodied in a non-disclosure Agreement and granted an enjoining order preventing the defendant from making use of the information provided by the Plaintiff under a NDA. However, the enjoining order was dismissed on technical grounds. At the time this case was instituted before the Commercial High Court of Colombo, the Section 160 of the IP Act of 2003 (discussed above) was not force and the basis of the action was on breach of contract. In the context of the provisions contained in the IP Act of 2003 the Plaintiffs in similar actions would be able to institute proceedings for an act of Unfair Competition under Section 160 of the IP Act of 2003.

Most companies, especially those developing software with unique features, seems to increasingly rely more and more on alternative measures such as the law of confidentiality to protect their products from possible infringement. The enforcement of these measure depend a lot on the ability of a court in a particular jurisdiction to give meaning and effect to contractual mechanisms used by companies to safeguard information shared with others (including employees). The additional features provided under Section 160 of the IP Act No. 36 of 2003 facilitate this to a great extent.

¹⁰ Directive 91/250/EEC

¹¹ Eg:- Northern Office Microcomputer vs Rosentein [1982] FSR 124

¹² H C (Civil) 156/2001 (1)

3.0 ELECTRONIC TRANSACTIONS

The Electronic Transactions Act No. 19 of 2006 was approved unanimously after debate by Parliament on 7th March 2006¹³ and certified by the speaker of Parliament on 19th May 2006. This finalized pursuant to a Joint Cabinet Memorandum of the Hon Prime Minister, Hon Minister of Trade, Commerce and Consumer Affairs and Hon Minister of Science and Technology. Consequently the Cabinet of Ministers authorized the draft legislation to be prepared by the Legal Draftsman's Department with legal and policy inputs from the ICT Agency of Sri Lanka (ICTA), ensuring that the draft legislation is in conformity with international standards & practices and the requirements of IT industry

The Legislation is based on the standards established by United Nations Commission on International Trade Law (UNCITRAL) Model Law on e-Commerce (1996) and Model Law on e-Signature (2001) and was brought into operation on 1st October 2007.

The preamble – *An Act to recognize and facilitate the formation of contracts, the creation and exchange of data messages 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*".

3.1 GENERAL FEATURES OF THE ELECTRONIC TRANSACTIONS ACT NO. 19 OF 2006

CHAPTER I of the Act

Section 2 describes the objectives of the Act 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.

CHAPTER II of the Act

The provisions contained in Sections 3, 4, 5, 6 and 7 together with the associated definitions for "data messages", "electronic document". "Electronic records" and "electronic signatures" are all based on the features contained in the aforesaid UNCITRAL Model Laws.

Section 3 of the Legislation 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 to give a wide connotation to all forms of electronic forms of 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.

¹³ Subject to a Committee stage amendment to Chapter V (Rules Governing Evidence)

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 manner in which information, required to be presented or retained in its *original* form, would be deemed to be satisfied, when it is in electronic form of 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.

The requirement for originality is found in numerous transactions such as quality and quantity certificates, inspection reports, insurance certificates etc. While such documents are not used to transfer rights or title, it is essential for such documents to be transmitted in its “original form” so that other parties in international commerce may have confidence in their contents. Section 6 goes beyond document imaging and it permits information to be retained in electronic form, regardless of whether or not the information is in the form of a paper document at the time it was first created.

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 of 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 introduce appropriate Regulations for the purpose of authorizing or facilitating and setting guidelines and procedures for the use of electronic communications or electronic records 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.

Section 9 provides for the legal recognition of the Government Gazette in electronic form. As per Section 10, the preceding sections would NOT confer a right on any person to insist that any Ministry, Government Department or Statutory body should accept or issue any document in the form of an electronic record or effect any monetary transaction in electronic form.

CHAPTER III

Section 11 to 17 deals with the legality and the modalities to engage in electronic forms contracting, including the recognition of an offer and acceptance in electronic form, attribution of electronic records, acknowledgment of receipt by the originator of a communication, time and place of despatch and receipt of electronic records and liability of network service providers for merely providing access. Whilst these sections were generally found to be aligned with the UNCITRAL Convention on the use of Electronic Communications in International Contracts, minor amendments were made to reflect the terms of the Convention.

Section 11 broadly provides for the recognition of an offer and acceptance of an offer expressed in electronic form a further provides 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 these rules to be effective there must be additional rules to ascertain 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. Section 12 to 14 achieves this objective.

Section 16 introduces exemptions for services providers and stipulates that a Certification Service provider shall not be subject to any civil or criminal liability for any transaction under the Act in respect of third party material in the form of Data messages, electronic records or communications, to which it merely provides access.

Section 17 (Avoidance of Doubt) clarifies the scope of Electronic contracting provisions and states *inter-alia* that “*the accepted principle of common law relating to contracts that the offeror may prescribe the method of communicating acceptance shall not be affected by anything contained in this Chapter*” and that “*a contract formed by the interaction of an automated message system and a natural person or by the interaction of automated message systems, shall not be denied validity or enforceability on the ground solely that there was no review or intervention by a natural person of the final contract or of each of the actions carried out by the automated message system*”

CHAPTER IV

Section 18 provides for the designation of a Certification Authority by Order published in the Gazette. Whilst Section 24 (2) provides for regulations to be promulgated specifying the powers, duties and functions of a person, body of persons or institution being appointed as a Certification Authority under Section 18, the scope and ambit of the powers which could be vested in such authority are confined to those stipulated under Section 19.

The provision for the accreditation of Certification Service Providers is contained in Section 20 and the criteria for accreditation of certification service providers, its cryptography services, electronic signature or advance electronic signature and security procedures and any associated legal benefits could be prescribed by Regulations under Section 24. The certificate of accreditation would be granted as per the provisions of the Sri Lanka Accreditation Board for Conformity Assessment Act No. 32 of 2005.

CHAPTER V

Whilst Section 22 excludes the application of the Evidence (Special Provisions) Act, No. 14 of 1995 to this Act, Section 21(1), (2) and (3) provides for a specific regime for the admissibility of any data message, communication, electronic document or electronic record and transactions under this legislation. The Committee stage amendment, introduced 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 and electronic records.

The rebuttable presumption in Section 21(3) provides that “*The Courts shall, unless the contrary is proved, presume the truth of information contained in a data message or communication, or in any electronic document or electronic record, and in the case of a electronic document or*

electronic record made by a person, that the electronic document or electronic record 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”.

CHAPTER VI

Section 23 excludes several categories of transaction from the application of the Act. These include, execution of a will, or any other testamentary disposition by whatever name called, a Bill of Exchange as defined in subsection (1) of section 3 of the Bills of Exchange Ordinance (Chapter 82); a Power-of-Attorney as defined in section 2 of the Power of Attorney Ordinance (Chapter 122); a Trust as defined in the Trusts Ordinance (Chapter 87) excluding a constructive, implied and resulting trust; and a contract for sale or conveyance of immovable property or any interest in such property. Section 23 (g) enables the Minister to exclude any other act or transaction from the application of this Act by regulations made under section 24.

The Regulation making provisions under Section 24 have been couched in the widest possible terms so that most of the administrative functions under the legislation could be prescribed by Orders published in the Gazette. Section 24 (1) states that the Minister would have the power to make regulations in respect of any matter required or authorized by this Act to be made, or for the purpose of carrying out or giving effect to the objectives of this Act, as specified in 24 (2).

3.2 E- TRANSACTIONS - CONCLUSIONS

Electronic Transactions Bill is an important piece of legislation for the overall development of ICT, electronic commerce as well as e-government activities in Sri Lanka. The Bill covers most issues usually covered under e-Transaction Legislation, except “*consumer protection*” issues, which are generally addressed through separate legislation.¹⁴

It should be noted that a new Legislation was introduced to enable transaction of cheques and negotiable instruments in digital form. This is facilitated through the Payment and Settlement Systems Act No. 28 of 2005, which was enacted with the Evidence (Amendment) Act No. 29 of 2005. The latter legislation has expanded the scope of the application of Section 90A of the Evidence Ordinance.

During the preparation of the Bill, UNCITRAL finalized and adopted the Convention on the use of Electronic Communications in International Contracts (see para 3.2 above). Whilst the Bill in draft form was generally aligned with the Convention, minor amendments were made to reflect the terms of the Convention.

The Bill has been identified as technology neutral and follows a **minimalist approach**, as regards the use of electronic signature, the legal structure and technical standards associated with the accreditation of Certification Service Providers, as confirmed by the UNCITRAL Secretariat.

¹⁴ This is an area on which International consensus has NOT yet been reached

4.0 COMPUTER CRIMES

The Computer Crimes Bill (LD-O 72/2000) was enacted by Parliament on 8th of May 2007 and certified by the Speaker of Parliament on 9th July 2007 as **Computer Crimes Act No. 24 of 2007**. This legislation is the result of contributions from CINTEC Committee on Law & Computers¹⁵ (1995-2000), Computer Crimes Sub-Committee of the Law Commission and the Ministry of Justice (2001-2006). It is being enacted at a time when significant strides are being made in the field of Information Communication and Technology development in Sri Lanka, through several initiatives such as the *e-Sri Lanka Development Project*¹⁶.

The Computer Crimes Act was brought into operation with effect from 15th July 2008.

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 to adapt 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.

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.

The Sri Lankan Computer Crime Act primarily covers 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 first class of offences in the Computer Crimes Act deals with Unauthorised Access to Computers and Information held in any Computer. The second class of offences deals with unauthorised modification and damage to a computer, computer system or computer program¹⁷. In addition a series of economic and national security related offences committed by means of a computer are also deemed to be offences under the Act.¹⁸

¹⁵ 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)

¹⁶ See www.icta.lk for details

¹⁷ 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.

¹⁸ Section 6 of the Act

With respect to Content related Cyber Crime (where Computers together with internet resources are used to distribute illegal data. Eg;- Internet based pornography, Criminal copyright infringement), 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 2006¹⁹ 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. In addition another

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.

Challenges

The Computer Crimes Act introduces a new regime for the investigation of offences under which ‘Experts’ could be designated to assist the Police in the investigation of offences under the Act. The powers and functions of an “expert” are explicitly stated in the Act. The introduction of the concept of an “experts” in the Act 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.

However, the challenge is to get the required regulations designating the said experts. 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 Act. The procedural laws have not been amended to facilitate the submission of affidavit evidence on matters concerning sensitive investigations.

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 records²⁰, admissibility is subject to several stringent criteria²¹.

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. If any Computer Crime committed arises out of an electronic based transaction, the admissibility provisions in the Electronic Transactions Act could be invoked in connection with the transaction. But this is an area requiring review and consideration.

5.0 DATA PROTECTION

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

¹⁹ New Sections 286B and 286C introduced through Penal Code (Amendment) Act No. 16 of 2006

²⁰ Evidence (Special Provisions) Act 14 of 1995

²¹ Eg – Certificate that the computer was working properly etc

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 democracy²².

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.

5.1 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 Act²³; 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 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 infrastructure²⁴. 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

²² See Bygrave, L., *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer, 2002.

²³ See <http://www.oic.thaigov.go.th/>

²⁴ See Chapter 5 on ‘Business Process Outsourcing Services for Economic Development’, pp.135-152, in UNCTAD *E-Commerce and Development Report*, 2003.

have been voiced in the European Parliament about the vulnerability of personal data being transferred under such outsourcing arrangements²⁵. Some view outsourcing as a process that effectively circumvents European regulatory safeguards. As a consequence, the Indian National Association of Software and Service Companies (NAASCOM) have recently been pressuring the Indian government to take some form of regulatory action to help forestall any regulatory reaction from Europe.

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 footing²⁶, 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.

5.3 The Data Protection Approach in Sri Lanka

The Government has directed ICTA 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 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. To mitigate the costs involved, however, the regulatory authority may not have an exclusively data protection remit. In South Africa, for example, privacy issues fall for consideration by the Human Rights Commission; while in Thailand, the Office of the Official Information Commission has responsibility for all aspects of public sector usage of, and access to, information.

²⁵ E.g. 'EU targets offshore data', *IT Week*, 13 April 2004.

²⁶ The presence or absence of a formal legal basis represents the key distinction between co- and self-regulation.

A sectoral regulatory response may be appropriate to address specific uses and abuses of personal data, whether driven by domestic or foreign concerns. In the telecommunications sector, many countries, such as Pakistan and Sri Lanka, have established regulatory authorities as part of an on-going liberalisation process within the sector, i.e. the Sri Lankan Telecommunications Regulatory Commission.

One of the stated functions of the Licensing Enforcement Directorate in the Pakistan Telecommunications Authority, for example, is ‘protects consumer rights and ensures privacy of the customers’²⁷. Also in the financial sector, nearly all countries maintain a distinct regulatory regime, which may address the protection of consumers of financial services, as well as the wider strategic economic aspects of the sector. These new or existing regulatory bodies may be capable of embracing data protection and privacy issues within their spectrum of duties.

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.

5.4 Codes of Practice

Codes of practice or codes of conduct (‘codes’) have traditionally been conceived as a body of rules providing guidance or setting down standards of behaviour, without the force of law. Codes are therefore seen as differing from public law instruments, such as statutes and regulations, and private law mechanisms, specifically contracts. However, although codes may be completely voluntary in nature, they may also be given a legal basis through legislation, contractual acceptance or judicial recognition. While a legal basis may not be essential to compliance with, and enforcement of, a code, where for example an industry body is able to exercise effective deterrent powers such as exclusion, it is likely to facilitate observance and enhance legal certainty for all parties concerned.

Codes 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 therefore 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, such as the Federation of European Direct and Interactive Marketing (FEDMA) ‘Code of Practice for the Use of Personal Data in Direct Marketing’²⁸.

In the Commission’s First Report ‘on the implementation of the Data Protection Directive’²⁹, it indicated disappointment at the number of such initiatives being pursued by the private sector, especially as “it believes that self-regulation, and in particular codes of conduct should play an important role in the future development of data protection in the EU *and outside*, not least in order to avoid excessively detailed legislation.” (emphasis added)(p. 26). The reference to the role of codes of practice outside the EU is a positive indicator in terms of the development of a Sri Lankan code.

²⁷ See <http://www.pta.gov.pk/ledirectorate/what.htm>

²⁸ <http://www.fedma.org/img/db/FEDMACodeEN.pdf>

²⁹ COM(2003) 265 final, 15.5.2003.

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 force³⁰. 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.

6.0 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.

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.

³⁰ 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.

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.

6.1 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.

11.0 CONCLUSIONS

Most legislative reforms require careful study and take several years to be enacted as legislation by Parliament. Therefore, a continuous review of the legal system is required to give legal effect to new developments in technology in order to facilitate the development ICT in Sri Lanka. Some of the recent enactments referred to above and other proposed changes are only an initial step in achieving this objective.