

THE LEGAL REGIME GOVERNING THE INFORMATION COMMUNICATION TECHNOLOGY IN SRI LANKA

K. A. A. N Thilakarathna*

Nisanka Jayarathne*

Introduction

ICT is made up of certain basic elements. The elements have all been present since the birth of the technology, but their relative significance and their visibility are still changing. The elements are automation, information, communication, integration, and sensation.¹The ICT sector includes computer hardware and software, tele communications, consumer electronics, and Internet-based contents, applications and services.²ICT stands for Information and Communication Technology, that is, technologies that store, transmit, and/or process information and communication. Although the term can be read literally to include all kinds of information-processing technologies, such as printing presses, Xerox machines, and abacuses, the term is generally used to indicate “modern” or “high” technology, electronic data-processing technologies.³The growth of Information Communication Technology (ICT) marks a revolutionary turn in the twentieth century. Compared to other

centuries, twentieth century is marked by rapid development in the areas of commerce, communication and globalization. The developments made in the ICT sector has had a propound impact on this rapid evolution from Alexander Graham Bell’s telephone to Sir Timothy John Berners-Lee’s World Wide Web.

This growth has brought dramatic changes by revolutionizing our customs and traditional methods of conducting business, communication and other activities which were based on paper methods. The days of analogy system with terrestrial transmitters are being rapidly overtaken by digital technology with satellite technology⁴.The ICT cluster of technologies emerged around the time of the Second World War and since then they have been the most important driver of global economic and social growth and change. Earlier clusters were based on textile machinery in the late 1700s, the steam engine (including railways and steam ships) in the early 1800s; electricity and steel in the late1800s; and

* Attorney -at- Law

lecturer in Law, Institute of Human Resources
Advancement
University of Colombo

Lecturer, Department of Legal Studies, Open
University

1P. Seipel, *Law and Information Technology: Swedish Views* (Swedish Government Official Reports, Stockholm 2002)

2M. Fransman, *The New ICT Ecosystem* (1st edn, Cambridge, CUP 2010), Preface

3J. Koops et al, *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners* (1st edn, T.M.C. Asser Press, 2006)28

4A.J. Mambi, *ICT Law Book* (1st ed, Mkuki Na Nyota, Tanzania 2010), Preface.

the internal combustion engine, oil and petrochemicals in the early 1900s.

According to Mambi⁵ ICT advances since the end of the 20th century have led to multiple convergences of content, computing, telecommunications and broadcasting. The development of ICT has led to significant social, economic and consequently legal changes. Technological change has one of its widest impacts on society and everyday life through ICT.⁶

The sheer impact of the new developments in the field of ICT necessitated for its proper regulation. ICT law can be identified as that branch of law which tries to regulate the ICT activities of a country. There are no fixed definitions for the term 'ICT Law'. According to Mambi, it can be briefly defined as, the legal subject that emanated from the development of technologies, the innovation of computers and other related devices, the use of Internet and Electronic Data Interchange (EDI), etc.

Law regulates technologies and solves conflicts and co-ordination problems related to those technologies. However, new technologies have had more powerful impacts on nature and on society and on our individual and organisational interrelationships with others. This means that there are also new risks, which must be managed. The new developments in Information and Communication Technologies have significantly affected the traditional legal concepts and brought about the necessity for the review and the reform of the law receptive to modern electronic dimensions. The role of the law is to recognise, regulate human conduct and

to enforce such regulation. Law is a method of technological risk management and plays a constantly increasing role in that regard. With the development of ICT, most of the traditional ways in which people used to engage in commerce and communication changed and with it came the instantaneous methods of doing things which would have otherwise taken much longer. However, with these advantages came many risks and disadvantages that needed to be managed as well. Today we speak of online transactions without paper money, and in the same time we also speak of cyber hacking and cyber theft almost like two sides of the same coin.

In considering the development of ICT in a Sri Lankan context, it can be said that we have been trend followers rather than trend creators in this arena. Sri Lanka has inherited many of its laws from the British and mainly in the areas of commercial law. Even after gaining its independence, Sri Lankan legislature was very reluctant to part ways with its British inheritance. Even regarding laws which have been enacted in the country regarding ICT have been influenced by the British tradition. Several enactments have been introduced to both take the advantages of the rapid growth in the ICT sector and to tackle the problems created with the boom of the same sector. Even though the ICT boom started to occur from the 1970's, Sri Lankan legislature did not take cognizance of the fact till the mid 1990's and it went on from there till the middle of the first decade of the new millennium.

5 *ibid*, Page 2

6T Pöysti, 'ICT and Legal Principles: Sources and Paradigm of Information Law' [2004] Scandinavian studies in law 560

International Legal Instruments Related to ICT

The development of information and communications technologies (ICTs) enables businesses and individuals to communicate and engage in transactions with other parties electronically, instantaneously and internationally. This gives rise to a variety of legal and regulatory issues for policymakers, from the validity of electronic methods of contracting and the security risks associated with them, to concerns over cybercrime and the ability to protect intellectual property rights online.⁷

There is a plethora of international legal instruments which have been implemented to regulate the ICT industry. Among them, and regarding electronic commerce, the United Nations Commission on International Trade Law (UNCITRAL) has made several initiations to develop conventions, model laws and guidelines related to the subject. UNCITRAL was established by the UN General Assembly by its Resolution 2205 (XXI) of 17 December 1966 with the ambition of promoting the progressive harmonization and unification of international trade law. The establishment of UNCITRAL was necessitated by the rapid increase in the volume of international trade which could no longer be managed with the domestic and regional laws which was capable of handling matters regarding international trade before this rapid expansion. UNCITRAL successfully adopted its Model Law on Electronic Commerce on

1996, Model Law on Electronic Signatures in 2001 and assisted to formulate UN Convention on Electronic Communications, adopted by the UN General Assembly in November 2005⁸.

Apart from commerce, there are other international legal instruments which focus on areas such as computer crimes and cybercrimes which could have serious implications on the national security of a country. The Budapest Convention on Cyber crime initiated by the European Union in 2001 The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. The preamble of the Convention declares that, its aim is to ‘pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.’⁹

Regarding data protection, the European Union in 2018 has taken new steps to protect data and the privacy of individuals. The General Data Protection Regulation (GDPR) 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas. GDPR has made some key changes to the existing EU law on the subject. The territorial applicability of the Directive is now expanded and whoever has personal data of

⁷United Nations, *Information and Communication Technology Policy and Legal Issues for Central Asia* (Guide for ICT Policymakers, UN 2007)

⁸Available at;<https://uncitral.un.org/>

⁹Preamble, The Budapest Convention on Cybercrime 2001

people residing in the EU comes under the jurisdiction of the Directive irrespective of the location of the company or the firm that holds the data. Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). The conditions for consent have been strengthened, and companies are no longer able to use long illegible terms and conditions full of legalese.

Sri Lankan Legal Framework on ICT

ICT is being developed at a tremendous speed and computer is the major invention or the result of the same. Law relating to ICT is not an isolated subject. Its involvement could be seen in any given area like criminal law, civil law, labour law, intellectual property law, taxation law and so on. However, as the subject is relatively new when compared to well established other branches of the private law such as Contract, Property and Trust, all of the parties need to come to a general consensus as to how they are going to work out and develop the advances in the ICT sector to both manage and regulate the same at both the international and domestic level.

ICT policymakers are constantly facing challenges in dealing with these issues. The promotion of harmonized law reforms, which would facilitate the sound development of e Commerce and related activities, that citizens have appropriate protection against harmful behaviour, is a way to address these challenges. An understanding of the legal issues involved remains of key importance to persons and organisations concerned with information and communications technology, and it is only armed with such understanding that they can satisfactorily address and cater for

the problems raised by the development and use of these technologies.

The Constitution of the Democratic Socialist Republic of Sri Lanka which was adopted in 1978 does not make any reference to the subject of Information Technology. Even under the directive principles it is difficult to find out any specific article which could be directly linked with the information technology of information communication technology in general. When one looks at the Nepalese Constitution of 2015 it makes direct reference to information technology under Article 51 of the Constitution which deals with state policy. Under Article 51 (F) dealing with the developmental policy, Article 51(F) (5) states that, 'developing and expanding information technology as required by the nation, and making its access easy and simple for the general public, while also making its maximum use for national development' shall be a State policy.

When one considers the ICT legal regime in Sri Lanka, there is no single coherent Act which is passed by the legislature. Instead there are several pieces of legislations which deals with several areas which are related to ICT. These legislations include, Telecommunication Act No 25 of 1991, Evidence (Special Provisions) Act, No. 14 of 1995, Information and Communication Technology Act, No 27 of 2003, Intellectual Property Act, No. 36 of 2003, Payment and Settlements System Act, No. 28 of 2005, Electronic Transaction Act, No.19 of 2006, Payment Devices Frauds Act, 30 of 2006, Computer Crimes Act, No. 24 of 2007, Right to Information Act, No. 12 of 2016.

The ICT legal regime in Sri Lanka consists of several legislations which have been

made with competencies of its own area of expertise. Much of these legislations have been influenced by foreign jurisdictions and United Kingdom has been often looked at. In order to understand the true value and effect of these legislations they must be evaluated on their own merit and afterwards the cumulative effect must be looked at.

Telecommunication Act No 25 of 1991

The Telecommunication Act No 25 of 1991 establishes the Telecommunications Regulatory Commission commonly known as the TRC. According to the section 04 of the Act, TRC have the main objectives of ensuring the provision of a reliable and efficient national and international telecommunication service in Sri Lanka, to protect and promote the interests of consumers, purchasers and other users and the public interest with respect to the charges for, and the quality and variety of telecommunication services, to maintain and; to promote effective competition between persons engaged in commercial activities connected with telecommunication, to promote the rapid and sustained development of telecommunication facilities both domestic and international, to ensure that operators are able to carry out their obligations for providing a reliable and efficient service, to promote research into and the development and use of new techniques in telecommunications and related fields, to promote the use of Sri Lanka for international transit services.

The objective of the TRC is a vital for establishing a good ICT infrastructure

regarding telecommunication. Country has seen a rapid increase in the use of telecommunication from 1991 to 2018. In 1991 there were only 125,834 fixed access telephone subscriptions and by December 2018 the number has risen to 2,484,616 nearly 20 times more compared to 1991. The alarming number is the cellular mobile subscription per 100 inhabitants which stands at 150 by December 2018 meaning that there are 1.5 mobile connections.¹⁰ The TRC uses a licensing system to control and regulate the telecommunication industry where it is made an offence under section 19 of the Act to operate a telecommunication system without a proper license. The relevant offences covered under the Act are included in part VI of the Act which deals with offences and punishments. Some of the offences include, fraudulent use of telecommunication service (sec 46), tendering false or fabricated messages (sec 48), wilful interception of telecommunication transmission (sec 53), transmission of unpaid message (sec 56) and tendering obscene or indecent or sedition message (sec 58).

In general, the Act can be appreciated for taking into consideration the ground realities of the early 1990's when the enactment was made. However, technology has developed rapidly and both the number of users and the devices have increased rapidly and in the contemporary world many telecommunication activities are not made through a telephone operator and are instead made using the internet through internet service providers. Therefore, the

¹⁰Available at

http://www.trc.gov.lk/images/pdf/statis_q42018.pdf

law needs to be updated taking this factor into consideration.

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

Before the enactment of the Evidence (Special Provisions) Act, No. 14 of 1995 computer evidence was not admissible in a court of law. This was clearly stated in the case of *Benwell v. Republic of Sri Lanka*¹¹ where it was held that, '[c]omputer evidence is in a category of its own. It is neither original evidence nor derivative evidence. Under the law of Sri Lanka, computer evidence is not admissible under section 34 of the Evidence Ordinance nor under any other section of the Evidence Ordinance.¹² With the development of technology and with advances in the mediums used to store data, Sri Lanka had to come up with legislations to make them admissible in a court of law and for that purpose the Evidence (Special Provisions) Act, No. 14 of 1995 was enacted. According to section 05 of the Act computer evidence are admissible in a court of law and section 02 makes it clear that the provisions of this Act are to be applied irrespective of whatever is mentioned in other legislations. Admissibility of computer evidence is a very important aspect in the ICT arena as ICT is mainly based on the works done using a computer. A computer is defined as 'any device the functions of which includes the storing and processing of information'¹³ under section 12 of the act. However, this term has not been judicially interpreted yet and the loose

11(1978-79) 2 Sri. L. R 194

12 (1978-79) 2 Sri. L. R 194

13It can be argued that according to this definition, even a washing machine could be

interpretation given to the term could be used to good effect by the judiciary.

It has nearly been 25 years since the enactment of this Act and some problems are still unresolved regarding computer evidence where the question as to whether things generated through modern communication tools and devices could be made admissible using the provisions of the Act. The question whether electronic messages could be used as evidence is still to be resolved by the apex Court of the country. Therefore, it can be said that admissibility of computer evidence under the Act in the modern context or in the world of internet is somewhat inadequate compared to the developments that have taken place since the enactment of the Evidence (Special Provisions) Act, No. 14 of 1995 nearly two and half decades ago.

Information and Communication Technology Act, No 27 of 2003

The Information and Communication Technology Act, No. 27 of 2003 is aimed establishing of an inter-ministerial committee on information and communication technology, providing for the formulation and approval of a national policy, providing for the establishment of the information communication technology agency of Sri Lanka with authority to develop and implement strategies and programmes on information and communication technology in both the public and private sector.

The Act does not have anything substantial and is mainly used as a policy generating

considered as a computer since it also has the capability of processing information

instrument. It is also a comparatively small piece of legislation as well. Sri Lanka first recognized the need for the development of ICT through the National Computer Policy (COMPOL) of 1983. The acceptance of COMPOL by the government gave rise to the establishment of the Computer and Information Technology Council of Sri Lanka (CINTEC) to function directly under the then President. The Information and Communication Technology Agency of Sri Lanka (ICTA) was established in July 2003 and pursuant to Information and Communication Technology Act No. 27 of 2003, (ICT Act), ICTA was identified as the legal successor to CINTEC and became the apex ICT institution of the Government. Under the ICT Act No. 27 of 2003 ICTA is empowered to formulate and implement strategies and programmes in both the Government and the private sector and pursuant thereto ICTA prepared programmes and strategies on Information and Communication Technology.

Intellectual Property Act, No. 36 of 2003

The Intellectual Property Act, No. 36 of 2003 was enacted as Sri Lanka was under an obligation to harmonize its laws according to the WIPO¹⁴ standards. As regards the protection of intellectual property rights (IPR), the Intellectual Property Act no. 36 of 2003 replaced the Code of Intellectual Property Act no. 52 of 1979. The IP Act of 2003 contains several new features in relation to the protection of software, trade secrets and integrated circuits. In the age of the internet traditional protection afforded to the IP rights may not be enough to afford the requisite protection. Specially with regards to patents, industrial

designs and copyrights are some of the important intellectual creations which warrants adequate protection in the age of the internet.

Integrated circuits are given separate protection under part VII of the Act. However, the real question of software protection under the IP Act is still unclear. Whether software could be afforded with patent protection or whether it could be afforded with copyright protections has not been answered. As the law stands, either way does not seem to be a real possibility. In the age of internet, Ip laws should be modified to afford the requisite protection that the respective IP rights.

Payment and Settlements System Act, No. 28 of 2005

Payment System is about how participants from individuals to banks, governments and international participants exchange monetary value within an economy and across national borders. It is the framework of laws, regulations, mechanisms, systems, procedures and agreements that governs payments. The Payment and Settlement Systems Act. No. 28 of 2005 (PSSA) provides for the regulation, supervision and monitoring of payments, clearing and settlement systems, the regulation of providers of money services and the electronic presentment of cheques in Sri Lanka. Payment Cards and Mobile Payment Systems Regulations No. 1 of 2013 (Regulation) provide Central Bank of Sri Lanka (CBSL) with the necessary authority to regulate service providers of payment cards and mobile payment systems in Sri Lanka. As per the provisions of the Regulation, no person can engage in the business or function as a service provider of

14World Intellectual Property Organization

payment cards or mobile payment systems except under the authority and in accordance with the terms and conditions of a license issued by the CBSL.

In the age of the Internet, credit cards and debit cards are more often used than paper money to make transactions and the 2013 regulation on payment cards and mobile payment systems have helped the ICT sector when it comes to both local and international commerce. Payment card refers only to debit cards, credit cards, charge cards and stored-value cards. Going further, regulation also makes provisions for mobile payment systems. The recent trend in international commerce has been to go with the mobile payment systems due to its convenience. Payment gateways such as Amazon and PayPal are two universally recognized service providers who contribute to billions of dollars' worth international transactions. Recently, the Central Bank of Sri Lanka formulated a mechanism for e-commerce payment providers to use multiple payment options for e-commerce/business transactions, within the current regulatory framework and they gave recent approval for 'Pay-Here', a payment gateway like PayPal.

For the most part, the above Act has helped the ICT sector in general when it comes to local and foreign trade and transactions. However, mechanism implemented under the Act does not allow individuals to make any claims to any institute in case where a service provider fails to satisfactorily treat a customer. This is an issue which would

need to be address if we are to really yield all the fruits of the Act.

Electronic Transaction Act, No. 19 of 2006

With the evolution of technology paper-based transaction soon started to fade away and it was replaced by electronic modes of exchange. Justice Saleem Marsoof states that '[t]he electronic evolution has transformed the way man does business and has brought about a great transformation in the law'.¹⁵ Kariyawasam¹⁶ states that, '[s]ignificant event in the legal regulation of e-commerce in Sri Lanka was the enactment of the Electronic Transactions Act in 2006'. She further states that, it is beyond dispute that Sri Lanka needs to embrace the enactment of the Electronic Transaction Act because this piece of legislation accords legal recognition to electronic commerce by ensuring the security and reliability of electronic communications. The world was brought closer together by the internet and it made vast changes in international trade which propelled 'globalization' through the expansion of the market and the reduction of the cost of access. The Act is a legal instrument which makes globalization a ground reality for Sri Lankans.

The Electronic Transactions Act, No. 19 of 2006 was enacted with the objective of facilitating domestic and international e-commerce and e-governance by eliminating legal barriers and establishing legal certainty, by encouraging the use of reliable forms of electronic commerce and promoting public confidence in the

15S. Marsoof, 'E-commerce & E-governance – Some Pertinent Issues' [2007] BALJ Vol. XIII 01 16K Kariyawasam, 'The growth and development of e-commerce: an analysis of

the electronic signature law of Sri Lanka' [2008] ICT Law 51

authenticity, integrity and reliability of data messages, electronic documents, electronic records and other communications. Section 04 of the Act makes it clear that, '[n]o data message, electronic document, electronic record or other communication shall be denied legal recognition, effect, validity or enforceability on the ground that it is in electronic form'. This is in line with the Article 04 of the UNCITRAL Model Law on Electronic Commerce. The recognition of electronic signature is also a salient feature of the Act. Section 07 recognizes that, an electronic signature is valid where law requires a signature and this almost repeals the requirement made out in the Section 18 of the Prevention of Fraud Ordinance No. 07 of 1840.

Section 11 of the Act states that, '[a] contract shall not be denied legal validity or enforceability on the sole ground that it is in electronic form'. This is a vital impetus for the ICT sector as it opens a plethora of opportunities to engage in commerce at the international level. In 2017 an amendment was brought to the Act and it was aimed to further expand the applicability of the Act regarding electronic transactions. Electronic Transactions (Amendment) Act, No. 25 of 2017 has brought the Sri Lankan electronic transactions legislation fully in line with the UN Electronic Communication Convention (ECC). Sri Lanka became the first country in South Asia and second country in Asia (after Singapore) to adopt the UN ECC standards. Sri Lanka ratified the UN ECC in July 2015. The amendment ensures greater legal certainty for e-commerce and e-business

17<http://www.dailymirror.lk/businessopinion/Major-boost-for-electronic-transactions-with-new-amendment/306-139137>

providers who wish to use the Sri Lankan law as the applicable law and ensure international validity for electronic contracts. It also ensures the legal validity for other international legal instruments as well as cross-border fund transfers, including enforceability of Foreign Arbitration Awards. The new legislation will improve trust and confidence and legal certainty for all types of business transactions using electronic means, thus improving competitiveness and ability to do business with greater efficiency.¹⁷ The new amendment strengthens the existing provisions to move government transaction to the digital era, through the use of stronger and more secure electronic-based authentication methods. Another unique feature of the amendment is that it facilitates electronic filing of any application, petition, plaint, answer, written submission or any other document in any courts.

Commenting on the Act, Ariyaratne¹⁸ As a developing country in Asian region, the Sri Lankan approach to the e-transaction is more progressive and closely reflects the international standards as well. Sri Lankan ETA has followed both UNCITRAL Model laws and ECC as well. Comparing to Indian approach, Sri Lanka has incorporated technology neutrality principle to more align with traditional contract law principles.

The Electronic Transaction Act, No. 19 of 2006 and its subsequent amendment can be appreciated for being timely and for incorporating the technology neutrality principle instead of a prescriptive approach.

18B Ariyaratna, 'Contracting in Cyber Space: A Comparative Analysis of Electronic Transaction Law in Sri Lanka' [2012] KDU-IRC

However, there are some gaps can be found in Sri Lankan law in relating to right to privacy and consumer protection in e-contracts. The Act is silent in regarding the consumer protection and right to privacy. As, Kariyawasam¹⁹ rightly pointed out, 'the Act recognizes that online transactions are valid but contains no specific provisions dealing with consumer protection'. Even though, the Consumer Affairs Authority Act No 9 of 2003 and Unfair Contract Terms Act No.26 of 1997 afford consumer protection for faced to faced contracts in some extent, those Acts also neglect to provide same protection for online contracts. Addressing this issue is of vital interest as even the latest amendment made to the Act has failed to address this issue.

Payment Devices Frauds Act, 30 of 2006

With the enactment of the Electronic Transactions Act, No. 19 of 2006 which made it possible to do electronic transactions, it then became potent to protect those who do engage in such transactions using electronic means and payment methods other than using printed money. With this objective in mind the Payment Devices Frauds Act, 30 of 2006 was enacted to, 'prevent the possession and use of unauthorised or counterfeit payment devices, create offences connected with the possession or use of unauthorised payment devices, protect persons lawfully issuing and using such payment devices, make provision for the investigation, prosecution and punishment of offenders'.²⁰

19K Kariyawasam, 'The growth and development of e-commerce: an analysis of the electronic signature law of Sri Lanka' [2008] ICT Law 51

Section 03 (1) of the Act lists out the respective acts which are deemed to be amounting to payment devices fraud. Some of Them include, embossing, encoding or skimming, making or altering equipment, unlawful use of phone listening device, providing track data to unauthorised individual setc. Section 3(2) stipulates the punishments for persons convicted of above-mentioned offences and the punishment runs from a maximum of 10 years imprisonment and a maximum fine of five hundred thousand rupees. The High Court is vested with the jurisdiction in relation to offences committed under the Act under section 19 and section 20 stipulates that these offences are cognizable meaning that granting of bail cannot be done without showing special circumstances for those who are accused of an offence falling under the Act. Further, section 17 stipulates that, any person who has the possession, control or custody any unlawful articles as mentioned in the Act shall be presumed guilty and till the contrary is proved the presumption will remain valid. This shifts the burden of proof from the prosecutor to the accused. Going still further, section 22 of the act offences committed under the Act are made extraditable offences.

This piece of legislation helps to complement the new opportunities created under the Electronic Transaction Act, No. 19 of 2006 which helped to expand the scope of trade and commerce in a digitalized era. This is a supplementary piece of legislation to the Electronic Transaction Act, No. 19 of 2006 where the

20Preamble, Payment Devices Frauds Act, 30 of 2006

Act supplements the electronic transactions by managing and regulating the modes of transactions used in electronic commerce.

Computer Crimes Act, No. 24 of 2007

Apart from providing a better way of life for society the rapid growth of ICT raises fundamental questions regarding storage of confidential information, privacy, data protection and crime. Computers are not only targeted for crime but are also important instruments used in the commission of other offences such as theft, fraud, forgery, damage, deletion of business information and sabotage of computer facilities, etc. The term “Computer Crime” is a generic term used to identify all crimes or frauds that relate to or related to computers and information technology.²¹The Computer Crimes Act No. 24 of 2007 provides for the identification of computer crimes and stipulates the procedure for the investigation and enforcement of such crimes. The Basis of the Computer Crimes Act No. 24 of 2007 is to criminalise attempts at unauthorized access to a computer, computer programme, data or information. Section 02 of the Act is very special as it allows to prosecute persons accused under offences under the Act irrespective of the fact whether they reside in Sri Lankan territory or not. The Act recognizes several offences related to computers which include securing unauthorised access to a computer, doing any act to secure unauthorised access in order to commit an offence, causing a computer to perform a function without

lawful authority an offence, dealing with unlawfully obtained data, illegal interception of data, using illegal devices and unauthorised disclosure of information enabling access to a service. The High Court is vested with the jurisdiction regarding offences committed under the Act under section 25. It is made an extraditable offence under section 27. Another innovative feature of the Act is the appointment of an expertise panel under section 17 to help in the investigation process regarding a computer crime.

Right to Information Act No. 12 of 2016

The Right to Information Act No. 12 of 2016 (RTI) was enacted to give effect to the Right to Information which was recognized a fundamental right under the nineteenth amendment to the Constitution which brought about the Article 14A giving a specific right to, right to information. Regarding the ICT sector and the related legal regime, RTI recognizes the validity of information kept in electronic means and the rights of the individuals to access that information which are kept in electronic means. The RTI also encourages keeping of new information in electronic formats as it would make it possible to give access to a wider range of audience who are seeking that information.

Moving Forward with the ICT Legal Regime

Translating policy objective into workable laws and regulations can obviously be a

²¹Available at;
<http://www.sundaytimes.lk/070729/FinancialTimes/ft308.html>

difficult task in any area of human endeavour; technology however presents particular challenges to law-makers, primarily due to the pace of change that occurs in the subject matter itself, e.g. software, computers and networks, and the manner in which such technology is utilized.²²

The Internet is the most striking example of the ICT revolution and the process of globalisation. Its immense popularity is shown by its millions of users all over the world. Our present Information Society is heavily affected by the Internet and the impact of this medium on everyday life will probably very much increase over the years to come.²³ With the technological developments in the new millennium ICT has become the benchmark where all most everything could be managed using the internet. With these new developments there also come the challenges associated with managing and regulating the virtual world. Many countries foresaw the challenges which would be posed with these developments and developed laws and regulations to face up with these new challenges. Germany is considered as the first country to adopt legislation on ICT.²⁴

In considering all the laws which have been enacted regarding ICT in Sri Lanka are in their totality are comprehensive. However,

issues related to use and implementation of those statutes have not been well founded and most of the lay people are not aware about them when compared to other laws. Two most important aspects regarding ICT law implementation are the principles of technology neutrality and pro-competitiveness. Technological neutrality is based on an acceptance that the environment is moving too rapidly to try and tie legal rules to a technology or market model. The principle, and variants of it, has been used in two key senses: that which is regulated off-line should be regulated on-line; as well as the need to treat different technologies similarly to the extent that they have the same effect²⁵. Pro-competitive principle states that, competition in the marketplace is accepted as the primary regulator of market participants, with governments intervening where market failures arise and to maintain fair competition.

When one considers Legal framework in Sri Lanka related to ICT it can be observed that most of the legislations which have been passed by the parliament are technology neutral. Legislations do not use many technical jargons to make it tech savvy. The Computer Crimes Act No. 24 of 2007 is a good example where this principle of technology neutrality is well preserved.

came as a bill in 1971 that together with the data protection acts of the German federal states and other area-specific regulations, governs the exposure of personal data, which are manually processed or stored in IT systems.

²⁵United Nations, *Information and Communication Technology Policy and Legal Issues for Central Asia* (Guide for ICT Policymakers, UN 2007)

²²United Nations, *Information and Communication Technology Policy and Legal Issues for Central Asia* (Guide for ICT Policymakers, UN 2007)

²³Michiel Brand, 'The Internet and the Law: An Article Examining the Problems and Questions Concerning the Regulation of Cyberspace' (2001) 9 TILBURG FOREIGN L REV 259

²⁴ The German **Bundesdatenschutzgesetz** (BDSG) is a federal data protection Act, which

The flow of information and goods across borders gives rise to international concerns over the enforceability and protection of intellectual property rights (“IPRs”), including copyright and related rights, patents and trademarks. However, regarding the pro-competitiveness, the ICT legal regime is below par. For an example, the Intellectual Property Act No. 36 of 2003 though a recent enactment, it lacks behind in many aspects. Protection of software under Sri Lankan IP law is problematic as neither patent law nor copyrights law can provide adequate protection. The IP Act does not even mention about software. It can also be observed that there is a slight mismatch between IP law and ICT regulation as the IP Act is not able to cope with the new developments in the ICT sector where the legislature has not given an enough interest to update its laws and regulations.

The IP Act is well equipped to protect traditional trademarks. However, when it comes to domain names which use names of trademarks the implementing procedure regarding protection of trademarks are not so well equipped to handle the matter in an age of the internet. There is no serious voice raised concerning these matters which are present under the ICT legal regime of the country.

It can also be seen that legal protection afforded to trade secret and confidential information under the IP Act in the age of the internet is inadequate as the IP act is more suited for the paper-based world rather than the paper less one. Security of information is an area which has developed very quickly and continues to develop a result of technological advances. This issue has not been satisfactorily addressed by the legislature.

The use of the Internet and electronic communications, with the ability to process large quantities of data, gives rise to significant concerns over how that data will be used, by whom and for what purposes. The law relating to data protection and privacy is almost non-existent in the country and this poses a serious threat for those individuals when their valuable personal information is held by others to be sold for a profit. In the age of the internet the ICT legal regime must address the issues related to data protection and privacy. The existing consumer protection laws are not adequate for the protection of consumer rights in an internet era in the country as they are both outdated and ill-equipped to handle matter arising from the internet or ecommerce. Sale of Goods Ordinance No 11 of 1896 and the Consumer Affairs Authority Act No 09 of 2003 are not amended or drafted in a manner which is conducive for protecting the consumers in an age of the internet.

In addition to the above, the implementation of rights, duties and obligations imposed under the several statutes which compose the ICT legal regime in the country is not well equipped to handle matters which arise in a tech savvy world in an efficient and effective manner. Most of the changes that have been brought about to the system in order to manage and regulate the ICT sector are underutilized and this is evident from the lack of decided cases by the apex courts in the country regarding computer crimes, payment frauds and even electronic evidence. Further, even if they had to be implemented it would have to be implemented in a judicial system already overburdened with so many other matters and disputes and without the required expertise

knowledge of the subject it would not be possible to think of a good outcome.

Conclusion

The ICT legal regime in Sri Lanka did not develop in the 1970s like in the more developed western countries or its Asian counterparts. For the most part, laws ICT sector started to emerge in the mid-1990s with the enactment of the Evidence (Special Provisions) Act, No. 14 of 1995 and the other related legislations which followed pursuit. The ICT legal regime therefore, consist of all these legislations which have been enacted in the age of the internet to both manage and regulate the ICT sector in fields such as telecommunication, electronic contracts and computer crimes. However, these legislations when compared to legislations of other developed countries are not well equipped to combat the misfortunes of the internet and related issues as the technology is moving way too fast when compared to these legislative initiatives. It is sad to see that the legislature has failed to take conscience recognition of the fact and they have not endeavoured to pass new laws or to amend the existing once to combat the issues which are brought up in the ICT sector. For an example, in the age of the internet, social media has become a prominent source of news and media where news spreads all over the world faster than fire. When the Easter attacks took place in April of this year where social media was fast spreading the news and some of it been hate speech all the government could do was to shut down the service providers by denying access without having a system to monitor and regulate the process by bringing the abusers to justice and therefore, denying the people who were within their bounds the rights to freedom of expression.

The ICT legal regime in the country fails to adequately provide solutions for the protection of data and privacy. Further its laws related to intellectual property fails to adequately protect the copyrights, patent rights and trademarks in an age of the internet. Another issue related to the ICT sector is the non-availability of a proper mechanism to combat cyber-crimes where the existing legislation on computer crimes is not adequate to combat issues related to cyber-crimes. Though we live in a digital world where it is all about e-literacy instead of literacy, Sri Lanka has not done well in this sector. For an instance where Sri Lanka has almost reached 96% in the country, the e-literacy rate is only 208%. Therefore, it can be said that even if we are to develop the ICT legal regime, we would not be able to have proper utilization of those reforms unless and until we improve the e-literacy of the individuals who will be dealing with them. In this context where the world economy is being dictated by the digital world, in order to move with its pace Sri Lanka needs to be contemporary with its laws, rules and regulations related to ICT.

Bibliography

- Ariyaratna, B. 'Contracting in Cyber Space: A Comparative Analysis of Electronic Transaction Law in Sri Lanka' [2012] KDU-IRC 39
- Brand, M. 'The Internet and the Law: An Article Examining the Problems and Questions Concerning the Regulation of Cyberspace' (2001) 9 TFLR 259
- Fransman, M. The New ICT Ecosystem (1st edn, Cambridge, CUP 2010)
- Kariyawasam, K. 'The growth and development of e-commerce: an analysis of the electronic signature law of Sri Lanka' [2008] ICT Law 51

Koops, J et al, Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners (1st edn, T.M.C. Asser Press, 2006)

Mambi, A, J. ICT Law Book(1st ed, Mkuki Na Nyota, Tanzania 2010)

Marsoof, S. 'E-commerce & E-governance-Some Pertinent Issues' [2007] BALJ Vol. XIII 01

Pöysti, T. 'ICT and Legal Principles: Sources and Paradigm of Information Law' [2004] Scandinavian studies in law 560

Seipel. P, Law and Information Technology: Swedish Views(Swedish Government Official Reports, Stockholm 2002)

United Nations, Information and Communication Technology Policy and Legal Issues for Central Asia(Guide for ICT Policymakers, UN 2007)

MANURAWA 2020