Final Year

Sri Lanka Law College

ICT Law

iGuide

Empowers Independent Learning

Independent Law Student Movement

Reviews, responses and criticism
iGuide,
Sri Lanka Law College,
244, Hulftsdorp Street, Colombo 12

Compiled by
iGuide Committee 2020

President
Nadeeshani Gunawardena

Co Secretaries
Arqam Muneer
Vivendra Ratnayake

Senior Committee
Nuwan Atukorala
Udani Ekanayake
Heshani Chandrasinghe
Rashad Ahmed
Nipuni Chandrarathne
Upeksha Perera
Ravindra Jayawardana
Nisansala Madhushani
Kavita Nissanka
Senandi Wijesinghe
Tehara Jayawardhana
Aranya Devanarayana
Poorni Mariyanayagam

Junior Committee
Osura Vindula
Dasuni Salwatura
Gayani Rathnasekara
Charith Samarakoon
Sharlan Kevin Benedict
Ashraf Mukthar
Marshadha Mackie
Amanda Chandrarathne
Vishwa Hewa
Uthpala Warusavithana
Githmi Ranathunga
Tameshiya Dahanayake
Chamalee Palihawadana

Special Thanks To:

Amali Charithma
Amanda Pabudunayake
Darshanie Miharanie Jayathilake
Deshan Peiris
Dilshi Wickramasinghe
Harindu Shehan
Hasthika Weerasinghe
Lahiru Weerasinghe
Lihini Dodangoda
Nimashi Pathirana
Pali Dewanarayana
Rozanne Chrisentia Irshad
Shani Fernando
Shenali Anthony
Thilini Jinendra

INTRODUCTION TO INFORMATION & COMMUNICATION TECHNOLOGY LAW

By **Sunil D.B.Abeyaratne**, *JPUM*, LL.M (London), MBA (IGNOU),
Diploma in Forensic Medicine & Science (Colombo), Attorney-at-Law, Int. Commercial Arbitrator,
Researcher-China-South Asia Legal Forum

Introduction

The Information Technology revolution has introduced the Computer and it has entered into most of the activities of the man during past few decades. Any Computer on the internet can access another computer on any network, e.g.ATMs withdrawal of money from an account from any place. With the development of Mobile Phone technology **m-Commerce** has been improved, e.g. Mobile banking, reservation of Air Tickets through mobile phone etc. All Computers related systems are vulnerable to intrusion and destruction. Perhaps, interruption of such system could lead to a total disruption of the daily life.

Trends are developing to shift nature of crimes from traditional to Hi-Tech. Computer may be used as a tool to commit a crime or storage. It is estimated that in near future, almost all the crimes in the world will be Computer related crimes and documents will be Computer based documents. Therefore, application of new methodology to investigate and seizure of data in Computer hardware, software, communication devices, computer peripherals or any other forms and storing of them are essential. Its forensic issues and introduction of new laws relating to Computer evidence play a vital role in forwarding Evidence before Courts of Law.

Main Areas of the Information Technology Law.

1. Computer Crimes
2. e-Commerce
3. Intellectual Property Rights
4. Employer-employee relationship under Information Society
5. Computer Evidence and its Forensic Issues.

Computer Crimes

<u>Computer crimes may be</u>

1. Computer related offences – accused used the computer/network as tool/s to commit offences.
2. Computer integrated offences – committed offences through computer/system/program
3. Contents related offence – change/destroy data introducing computer virus/worm etc.

<u>Why we cannot deal Computer based offences with existing and traditional criminal offences ?</u>

E.g:- Main ingredient to fulfill the offence, `Theft' is involvement of movable property (which is tangible). *Oxford vs. Moss [1978] 68 Cr.App.Reports 183 for* See for Intangible property involved in Theft of *Data*. See *Cox vs. Riley (1986) 83 Cr.App.R 54* for involvement of valuable article under Criminal Damages Act in UK.

Computer based main criminal offences –

a) unauthorised access to (computer hacking) any computer or information held in any computer.
b) the offence of unauthorised access with an intention to commit further offence (computer cracking). Mere turning on a computer is sufficient to fulfil access to any computer and it is not necessary to have unauthorised access directed at any particular programme, data or computer, to access information held in any computer.
c) causing a computer to perform a function without lawful authority and same will result in unauthorised modification or damage or potential damage to any computer, computer system or computer programme. Transmitting of virus to another organisation accidentally or negligently may be offences under this section.

See Articles 2-11 of the Convention on Cybercrime (Budapest)

Various jurisdiction have introduced the following computer based criminal offences,

- offences committed against national security, the national economy and public order causing a computer to perform a function,
- obtaining information without lawful authority from a computer or a storage medium of a computer buys, receives, retains, sells or in any manner deals with or offers to buy or sell, or in any manner deals with or downloads, uploads, copies or acquires the substance or meaning of as and offence and sentence for the same.
- illegal interception of data
- using of illegal devices
- unauthorised disclosure of information enabling access to a service as an offence.
- Attempt to commit the aforesaid offences also as offence

Special provisions for investigations on Computer based offences such as issuing of warrants, seizure of articles and preserving them, appointment of experts to carryout investigations etc. introduced under these laws. Special provisions for international cooperation to seize, preserve, produce and investigate data in relation to computer crime also introduced into domestic laws of the countries..

<u>Other Computer based offences</u>

Publication of an obscene article is a criminal offence under Obscene Publication Acts. Storing or distribution of child phonographs by e-mail and the Internet is also an offence Employer (negligent director or manager or company) also may be prosecuted for the offence committed during the employment of the employee.

Electronic Commerce

Principles relating to `Offer' and `Acceptance' under Law of Contracts are applicable for e-transactions as well. Only difference is the medium of transactions. In e-Commerce, medium is electronic media.

Postal theory under the Law of Contracts (of sending mail) cannot apply for sending of e-mail. When the message received by the Service Provider of the Receiver or soon after the sender lost his control over the electronic message it presumes that the receiver received the message. This is important considering the nature of travelling electronic messages from one place to another.

<u>On-line transactions.</u>

Message on the Computer screen is only an Invitation to treat and not an offer. Computer operator has to offer and the same will be accepted by the advertiser.

<u>Mode of Payment</u>

After giving secret number of the Credit card to make the payment then and there the agreement will be completed.

<u>Electronic Transactions / Commerce Act</u>

No 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.

Intellectual Property Rights

Intellectual Property Laws provide copy right to computer programs following TRIPS and WIPO Convention. Patents and design rights are also available for the same. Some IPR violations in cyber space are,
Copyright violation - illegal copying, downloading and uploading of files etc
Patent infringement
Unfair Competition – mouse trapping, Linking, Framing, Spamming etc

Employer-employee relationship under Information Society

As far as the said changes in the Information Society is concerned, it is not fair one to expect the employer to maintain and stick into traditional environment or methods like paper based documentation or sending letters through postal service without application of modern technology. However, the adjustability or suitability to the conversion of a working place from traditional system into a modern environment under Information Society can be a serious problem.

In any given Employer-employee contract, there may be both express and implied terms govern the same contract. Most of such contracts prepared for working places influenced with new technology have included express flexibility and mobility clauses to face new challenges in any given trade or business.

In general, it is the duty of the Employer to provide necessary training to get the employee/s' competence and adjusted to new working conditions.

There should be a mutual consent between Employer and employee to update applicability of the necessary skills, or knowledge of the employee for the establishment and to provide necessary guidance and training by the Employer to improve the same skills of the employee.

If the employee is purposely refusing to gain necessary knowledge and show skills can lead to a fair dismissal.

Under the normal principle of vicarious liability, Employer may be liable for the actions of his employees during the employment and the Employer has to pay damages on such occasions for the employees' action. Further publication may be far wider through e-mail and Internet due to its nature and same can be damaging more to the victim in defamation case and will tend to increase the damages.

Internet Service Provider (ISP) will be liable primarily as a publisher of defamatory statement of a third party, when ISP carries the same on its server a news group even the employee of the ISP were ignorant of a defamatory material. Even a publication is expressly prohibited, if the employee as author and acting in the course of his employment or for the purpose of the employer's business publishes the same publication, the employer also may be liable upon vicarious liability.

Like sexual harassment, racial harassment through e-mail is another aspect in Information Society.

Due to the nature of e-mail and Internet Communication, news groups, chat rooms etc., can create its own problems and a company is generally identified as the origin of e-mails and not the employee of the same company. Monitoring of emails and internet downloads and uploads during the working hours of the establishment is important in Information Society.

Nature and Discovery of Electronic Evidence

Computer evidence may be stored in hidden files as there is a great deal of left over data stored on their disk drives of a computer and some institutions may store their data at a distant server, different website, computer clouds etc.

Discovery of evidence is the most essential part to prove a case and various jurisdictions have faced common and different types of difficulties unique to relevant legal systems due to its own nature (of laws), procedures etc. When the subject matter discussed with

`electronic evidence', it will be a more complicated issue compared to discovery of non electronic evidence. With development of technology, evidence takes a new form and e-mail, chat room transcripts, databases, spreadsheets, web browser history files, information through system backup tapes have been replacing conventional paper documents.

Digital discovery tends to be voluminous, as electronic data are easier to copy, archive and distribute. Electronic data, unlike their conventional counterparts, do not disappear easily and difficult to actually, delete and destroy of an electronic document. Cost factor relating to digital discovery is also a serious problem due to its nature. Privacy issues is another aspect under Digital discovery since courts can allow access to email, records of Web sites visited, transcripts of chat room discussions etc. to discover such evidence.

Standard of knowledge and competence of investigators and their ability to explain the relevance of electronic forensic and powerfulness of the forensic analysis tools use for discovery of electronic evidence also might open doors for different level of acceptability of such evidence in Court trials. It is the duty of the Forensic experts to ensure that nothing has been added to or deleted to electronic evidence recovered from the scene of crime/place.

In general, opposing party is allowed to request relevant material from the proposed party to produce of such evidence. However, one cannot apply rules relating to traditional discovery methods as it is for discovery of electronic evidence due to its nature, e.g.discovery of electronic evidence may be time consuming, expensive, involved in rules relating to privileges.

As far the nature of Digital Discovery is concerned, one has to face number of problems. Considerable number of institutions in the world stores their documentation in digital form on computers. They keep communication through e-mail, electronic voice mail systems etc. using Computers. As a result burden of proof of such evidence also can be complicated, e.g. Reconstructing, restoring, and searching data.

These matters were discussed in number of International Conferences and the International Community is still struggling to remove uncertainty regarding same. It is clear that new discovery approach must be introduced globally to maintain uniformity among all Nations to minimise the said practical problems.

Different countries have adopted different policies upon IT related evidence. Due to the nature of this type of evidence any particular country cannot apply restricted laws and rules relevant to their territories. Electronic data always freely flow crossing boarders of the States. Management methods of documents in digital form may be different from one country to another. Storing of data is another aspect and we have to consider whole world as one jurisdiction considering the ways electronic records are saved.
See the objective of the Convention on Cybercrime.

****