News_BMFE_2000-44.pdf

03/06/00 Daily News

Can our legislative infrastructure support a successful E-commerce?

by Krishanie Swaris Fernando

E-commerce constitutes an international rubric into which must be filled in the national requirements. This recognition must extend to the legislative regime and also to its practical implementation.

To achieve this transition one would have to consider a shift or a parcel shift from a legal framework which traditionally relies on paper based legal procedures and requirements designed for the physical world to a cyber based paperless, faceless and virtual world that defies traditional concepts of time and space.

At local levels new laws are being envisaged and proposed or enacted with the objective of ensuring access to the cyber market and building trust and confidence in the legal system.

Consequently a predictable, transparent, and flexible legal environment would be a policy goal.

At international levels the UNCITRAL Model Law on Electronic Commerce (1996), ICC guidelines, OECD guidelines and principles and the EU Directives and other initiatives may be referred.

Why regulate

The success of e-commerce will depend on the legislative infrastructure. An unregulated e-economy may promote a lawless frontier threatened with e-crime leaving the e-consumer without justice and redress.

Identifiying emerging legal issues

Datasecurity

For successful e-commerce an electronic transaction has to be legally binding and must meet certain fundamentals; 1) sender authenticity, 2) message integrity, 3). non repudiation by the sender or the recipient of the message resulting in admissibility as evidence and 4). Message security extending to cope with the risk of hacking or masquerading, message corruption or loss.

Public-key cryptographic technology is currently widely recognized as an essential tool for creating a secure e-transmission, while the verification of the authenticity and integrity of the data and the identity of the signatory may be confirmed by a Certification Authority (CA) by the issue of a digital certificate. The CA acts like a trusted electronic Notary.

Some of the legal issues which will arise from such developments and will have to be addressed by way of legislation are:- 1) is an electronic transmission a writing ? 2) what constitutes a signature within an electronic transmission? 3) the legal identity and liabilities of the CA ? 4) the regulations governing the certificate issued by the CA ? 5) would the retention of documents in electronic forms suffice?

These issues may have to be addressed in the light of the Prevention of Frauds Ordinance of 1840 which is a main obstacle to the paperless e-commerce, which states that "No promise, contract, bargain or agreement unless it be in writing and signed by the party making the same, or by some person thereto lawfully authorised by him or her, shall be of force or avail in law....." Also other Enactment's containing and defining the words "Document" "Writing" "Instrument" "Signature" and the Interpretation Ordinance may have to be addressed.

Internationally DIgital Signature Statutes have been enacted in many states of the USA. Some are technologically specific (Utah model), some are technologically neutral (California model) and others are a hybrid of different approaches (Illinois model). In 1998 the Singapore Electronic Transactions Act was followed in 1999 by the Singapore Electronic Transactions (Certification Authority) Regulations. Likewise there are laws in Canada, Australia, New Zealand, Malaysia, South Korea, and many of othe EU countries.

The UNCITRAL Draft Uniform Rules on Electronic Signatures, the OECD's work following upon its 1997 cryptography policy, the EU Directive proposal for a common frame work for e-signatures, the ICC guide lines known as the General usage for International Digitally Ensured Commerce (GGUIDEC) may be referred.

Data privacy

Key to confidence building in a networked environment if people are to engage in e-commerce is the need for Data Protection (DP) legislation.

DP Legislation governs the manner in which computerised data relating to individuals may be collected, held, processed, used, disclosed and transferred internationally.

It seeks to curtail the collection and abuse of extensive, unauthorised and individualised information of the user of the internet.

Globally the EU Directive 95/46/EC on DP may affect trans board flow of data to a Third Country which does not have adequate DP laws.

Sri Lanka does not have any specific DP legislation. The effect of this Directive to Sri Lanka is that we may not be able to export or import personal data to or from Europe unless it falls within the exceptions to the prohibition on transfer. A further possibility which is already in use in many countries is to enter into trans border data flow agreements.

The US approach includes sector specific legislation, regulation, private sector codes of conduct.

Consumer protection

Essentially the consumer will resort to e-commerce only if there is a sound legal safety net.

The Consumer Protection Act No. 1 of 1979, the Consumer Credit Act No. 29 of 1982, the Unfair Contracts Act and many other related acts have not been fashioned to accommodate the Cyber consumer and will have to be addressed.

Also e-commerce will not develop without a secure and legally binding electronic payment system. Fraudulent use and counterfeiting are serious concerns. Exchange control laws will also have to be addressed.

Laws on electronic Contract formation will also have to be addressed.

According to the OEDC guide lines for consumer protection in on-line commerce - on line shoppers should be afforded effective protection that is not less than protection afforded off line. The EU Directive on distance selling and contract formation may also be referred.

Intellectual property

The transition from the protection of traditional information to the protection of open public global networks such as the Internet will need consideration for new laws.

Liability of service providers, e-mail operators and other intermediaries for the content and conduct of e-commerce sites may have to be accommodated.

Also the legal implications of digital manipulations such as morphing, framing, meta tagging, hyper fiction, cookie, spanning, browsing, mirror sites etc. may have to be considered.

As such the uncertainties which surround the electronic dimensions of Intellectual Property Laws will seriously hinder e-commerce development since commercially important information will be withheld from uncertain methods of distribution and the theft of piracy threaten a successful e-commerce. In this light the Code of Intellectual Property Act will have to be addressed.

Internationally the effective implementation of the WIPO Copyright Treaty and the WIPO Performers and Phonograms Treaty adopted in 1996 is an effort to raise a minimum standard particularly with respect to net work based delivery of copyright material.

Development of e-commerce would also depend upon the encouragement and protection of the patentable innovations in the fields of computer technology including computer software, computer hardware, telecommunication etc.

A trade mark is a vital aspect of trading on the web. However trade mark clashes are beginning to appear on the Internet. For instance since very few companies may have their trade marks registered in all countries an advertisement put on the internet in one country by the owner of that mark in that country may infringe the registered trade mark of another country which has it registered in that country in which the advertisement is accessed and read.

Domain names are the new branding issue which arises with internet commerce. There are many instances where famous trade marks are misappropriated as domain names by third parties eroding the value of the mark and misleading the consumer and domain name piracy. These new issues must be addressed. In 1997 a body known as the International Ad Hoc Committee (IAHC) proposed for private registries to allocate domain names and also proposed a dispute procedure using the WIPO arbitration procedures.

Evidence

The whole concept of a legal e-commerce may fall apart for the lack of practical administration of electronic evidence. The Evidence Ordinance nor its amendments facilitate e-commerce and may have to be addressed.

It must be noted that evidentiary difficulties may arise in proving the existence of events in cyberspace because of its transient and intangible nature.

Jurisdiction and conflict of laws

The Internet commerce poses unique jurisdictional difficulties for courts around the world because e-commerce orders, e-mails, web posting, downloads, leap from computer to computer with no regard for national borders. Also the Enforcement of such a judgement would necessarily not follow.

Faced with a transboundary nature of the internet contract and problem of admissibility of evidence the alternate dispute resolution mechanisms such as arbitration, mediation or expert determination may have to be considered.

Electronic crime

A Computer Crimes Act is a crying need if e-commerce is to be successful. The Council of Europe has stipulated a minimum list of computer related offences necessary for a criminal policy ie-Computer Fraud, Computer forgery, Damage to Computer Data or Computer Programs, Computer Sabotage, Unauthorized Access, Unauthorized Interception.

Tax

The traditional system of taxation based on a physical presence within a tax jurisdiction has been jettisoned by the e-commerce revolution. The potential speed, un-traceability and anonymity of e-transactions providing digitized goods and services may create new possibilities of tax avoidance and evasion.

Ideally for e-commerce to develop the tax obligations must be clear, transparent and predictable and no extra burden be imposed compared to the traditional commerce.

The tax regime to regulate e-commerce is being hotly debated in some countries. The US have decided not to impose any tax on e-commerce for the first three years. The OEDC has undertaken to draw up a global program on electronic commerce regulation.