

Adequacy of cyber laws across the world

Sunil K. Bahri,

Principal Director International Relations

Office of the Comptroller and Auditor General of India

1. Background:

The use of Information Technology for the conduct of trade transactions has been increasing rapidly and was expected to develop further as technical support become more widely accessible. However, the legal validity of information in electronic form has always been questioned. A need was, therefore, felt for a Law on Electronic Commerce. In order to offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for "Electronic Commerce", the United Nations General Assembly in December, 1996 adopted a model Law on e-commerce titled 'UNCITRAL Model Law on Electronic Commerce'.

2. UNCITRAL Model Law on Electronic Commerce:

This model law attempts to address some concerns regarding electronic transactions. Some of the more important ones are:

a) Legal recognition of data messages (Article 5)

Article 5 embodies the fundamental principle that data messages should not be discriminated against, i.e. that there should be no disparity of treatment between data messages and paper documents.

b) Writing (Article 6):

Article 6 is intended to define the basic standard to be met by a data message in order to be considered as meeting a requirement (which may result from statute, regulation or judge-made law) that information be retained or presented "in writing" (or that the information be contained in a "document" or other paper-based instrument).

c) Signature (Article 7):

Article 7 adopts a comprehensive approach with a view to ensuring that a message that was required to be authenticated should not be denied legal value for the sole reason that it was not authenticated in a manner peculiar to paper documents. It establishes the general conditions under which data messages would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements, which currently present barriers to electronic commerce. Article 7 focuses on the two basic functions of a signature, namely to identify the author of a document and to confirm that the author approved the content of that document.

d) Original (Article 8):

Article 8 should be regarded as stating the minimum acceptable form requirement to be met by a data message for it to be regarded as the functional equivalent of an original. The provisions of article 8 should be regarded as mandatory, to the same extent that existing provisions regarding the use of paper-based original documents would be regarded as mandatory. The indication that the form requirements stated in Article 8 are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

e) Admissibility and evidential weight of data messages (Article 9):

The purpose of Article 9 is to establish both the admissibility of data messages as evidence in legal proceedings and their evidential value. Data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form, it puts emphasis on the general principle stated in article 4 and is needed to make it expressly applicable to admissibility of evidence, an area in which particularly complex issues might arise in certain jurisdictions.



f) Retention of data messages (Article 10):

Article 10 establishes a set of alternative rules for existing requirements regarding the storage of information (e.g. for accounting or tax purposes) that may constitute obstacles to the development of modern trade.

g) Formation and validity of contracts (Article 11):

Article 11 is not intended to interfere with the law on formation of contracts but rather to promote international trade by providing increased legal certainty as to the conclusion of contracts by electronic means. It deals not only with the issue of contract formation but also with the form in which and offer and acceptance may be expressed.

h) Recognition by parties of data messages (Article 12):

Article 12 was added at a late stage in the preparation of Model Law, in recognition of the fact that article 11 was limited to dealing with data messages that were geared to the

conclusion of a contract, but that the draft Model Law did not contain specific provisions on data messages that related not to the conclusion of contracts but to the performance of contractual obligations (e.g., notice of defective goods, an offer to pay, notice of place where a contract would be performed, recognition of debt).

i) Attribution of data messages (Article 13):

Article 13 is intended to apply where there is a question as to whether a data message was really sent by the person who is indicated as being the originator.

j) Acknowledgement of receipt (Article 14):

The provisions of article 14 are based on the assumption that acknowledgement procedures are to be used at the discretion of the originator. Article 14 is not intended to deal with the legal consequences that may flow from sending an acknowledgement of receipt, apart from establishing receipt of the data message.

k) Time and place of dispatch and receipt of data messages (Article 15):

The Model Law is intended to reflect the fact that the location of information systems is irrelevant and sets forth a more objective criterion, namely the place of business of the parties.

3. Concern of SAIs:

As Governments and other agencies under the audit jurisdiction of SAIs switchover to IT environment, several crucial issues regarding evidence, authentication of documents, power of investigations, management of records etc. arise which impact the functioning of the auditor. Furthermore, any deficiencies in law would also act as a barrier to realising the full potential of IT applications. It was with this view that a study was undertaken by SAI-India to ascertain the extent to which the important provisions of Model Law were incorporated in the Laws of various countries.

SAI-India devised a questionnaire incorporating various provisions contained in the Model Law and seeking information from SAIs as to the extent to which those provisions were included in the legislation of their countries. Out of 185 SAIs which were queried, responses have been received from 44. While 24 SAIs stated that there was no separate IT Law, 20 SAIs (Australia, Austria, Brunei Darussalam, Canada, Chile, Egypt, India, Israel, Japan, Lithuania, the Netherlands, Norway, Pakistan, Peru, Poland, South Africa, Slovakia, Slovenia, Ukraine and United Kingdom) responded to the questionnaire.

4. Deviations from UNCITRAL:

Analysis of the responses revealed that most of the important provisions of Model Law were incorporated in the IT related Laws of countries. However, there were deviations, which are discussed below:

Legal recognition of data messages (Article 5):

The above provision was not incorporated in the Laws of Chile and Netherlands and it was partially incorporated in the Laws of Canada and Lithuania.

Writing (Article 6):

The provision was not incorporated in the Law of Poland and it was partially incorporated in the Laws of Canada, Chile, Lithuania and Netherlands.

Original, Legal acceptance of electronic records (Article 8):

The provision was not incorporated in the Law of Poland and it was partially incorporated in the Laws of Australia and Netherlands

Admissibility and evidential weight of data messages (Article 9):

Partially incorporated in the Laws of Canada, Chile, Netherlands and Poland.

Retention of data messages (Article 10):

The provision was not incorporated in the Laws of Chile, Egypt, Israel and Poland

Formation and validity of Contracts (Article 11):

The provision was not incorporated in the Laws Australia and Egypt and it was partially incorporated in the Laws of Chile, Israel, Pakistan and Peru.

Recognition by parties of data messages (Article 12):

The provision was not incorporated in the Laws of Chile, Egypt and Israel and it was partially incorporated in the Laws of Canada, Pakistan, Peru and Netherlands.

Attribution of data messages (Article 13):

The provision was not incorporated in the Laws of Chile, Egypt and Israel and Poland and it was partially incorporated in the Laws of Canada, Lithuania, Pakistan and Netherlands.

Acknowledgement of receipt (Article 14):

The provision was not incorporated in the Laws of Chile, Egypt and Poland and it was partially incorporated in the Laws of Canada, Australia, Israel and Peru and Netherlands.

Time and place of dispatch and receipt of data messages (Article 15):

The provision was not incorporated in the Laws of Chile, Egypt and Poland and it was partially incorporated in the Laws of Israel, Peru and Netherlands.

5. Other significant matters:

- Laws of Australia, Lithuania, Poland and South Africa provide for Electronic Signature without specifying technology.
- In the Law of Austria, electronic transactions using Digital Certificate were allowed for transactions with Government only.
- In the Laws of Canada, Japan and Australia there was no clause for recognition/licensing of Certifying Authorities.
- The cost of obtaining Digital Certificate by a subscriber from a Certifying Authority was not fixed in any of the countries except Peru.
- There was no separate authority to deal with offences under the IT Laws of Norway, India, Chile, Egypt, Brunei Darussalam, Netherlands, Pakistan, Poland, Japan and Peru.
- The Laws of Austria, Brunei Darussalam, Pakistan and Peru does not provide for copyright and related offences as criminal offences, which involve reproduction and distribution by means of a computer system, or works protected by copyright.
- The Laws of Canada, Chile, Netherlands, Japan and Peru do not give special powers to the Government for dealing with Cyber crimes.

6. Cyber Laws on website:

Some cyber laws have been posted on the website of the Comptroller & Auditor General of India www.cagindia.org. These are Uniform Electronic Commerce Act of Canada, Computer crimes Act, 1997 & Digital Signature Act, 1997 of Malaysia, Electronic Signature Regulations, 2002 of United Kingdom and the Information Technology Act, 2000 of India.

7. Conclusion:

From the information available it appears that but for some deviations most legislation on IT across the world has addressed major concerns. The SAI fraternity will be well advised to familiarise themselves with the main legal issues involved in IT and the legislation of their respective countries. Compliance to IT legislation would also be an important factor for consideration while auditing in an IT environment.