Bharat's Cyber and E-Commerce Laws

Edited by **S/Shri Parag Diwan,** Dean & Director, AIMA-CME, New Delhi AND **Shammi Kapoor,** Advocate Price Rs. 595/-

P.S.N Prasad
Asstt. Legal Adviser

Though the widespread use of Internet and related technology and consequent explosion of electronic commerce has became the order of the day, the fundamental question before us is whether appropriate legal and regulatory framework exists to govern such business in India and the third world countries. Further, in the case of electronic commerce transactions, what are the mechanisms for resolution/redressal of disputes. With the recent enactment of Information Technology Act, many of these issued are addressed by the Act in India.

Bharat's **CYBER AND E-COMMERCE LAWS** edited by Shri Parag Diwan and Shri Shammi Kapoor, deals with the existing scenario of Cyber and E-Commerce Laws and is published by Bharat Law House Pvt. Ltd., T-1/95, Mangolpuri Industrial Area, Phase I, New Delhi-83. The editors of the book under review have said that this book is an attempt to demystify many of these issues as well as technological background behind them. The contents of the book are divided into twelve chapters. The first two chapters look into the transformation of our society into an information oriented one and the interplay of information gathering techniques with the legal and regulatory environment. The next four chapters look into the concepts of theft of information and data protection.

The authors have extensively dealt with the pinciples of data protection. Chapters seven and eight deal with copyright issues relating to information technology and the nature of copyright protection vis-a-vis software and information technology services. In the ninth and tenth chapters, the issues relating to individual privacy and how information technology aided surveillance can intrude upon an individual's right and how they are protected are dealt with. The editors deserve appreciation for the key chapter penultimate which discusses various aspects of transactions such as those creating binding commitment, enforceability of the agreement, electronic fund transfer and digital signatures. In the twelfth chapter, the editors have dealt with the menace of computer hacking and the provisions in law that safeguard ones information system against hackers attack. The book contains an appendix that provides a complete text of Information Technology Act, 2000.

In the preface the editors have stated that the legal issues associated with Electronic Commerce arise from three major aspects of Electronic Commerce and are as follows :

(i) The evidentiary and authentication issues associated with the elimination of or absence of paper, and its replacement by electronic records.

(ii) changed relationship with trading partner arising from the changes in business or trading practices that are so often accompany Electronic Commerce (e.g., shortened timeframes, elimination of certain documents, use of databases.

(iii) The new business and contractual arrangements that are entered into with providers of the solution elements of Electronic Commerce (e.g., Value Added

Network Services Providers, Software Providers, Others Service or Solution Providers).

The legislation on Computer/Information Technology was passed on 17th May 2000. This law adopts the model law on Electronic Commerce adopted by United Commission on International Trade Law and it aims at amending the Indian Penal Code, Indian Evidence Act, 1872, the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto (Page 34).

In Chapter 3 (Theft of information), the editors have discussed the applicability of definition of 'property' in terms of Theft Act, 1968. The property rights in information have been discussed with the help of the renowned case **Oxford v. Moss.** Mr. Moss was a student at Liverpool University. In a manner unfortunately not disclosed in the Law Report, he discovered and removed a proof copy of an examination paper which he was due to sit. His plan was to copy the contests of the paper and, being aware that if the paper were discovered to be missing a replacement paper would be set, to return the paper to its original location. Upon his conduct being discovered the question arose as to whether any criminal offence has been committed. As it was an integral part of his scheme that the original paper should be returned, it was considered that he could not be charged with the theft of the paper. A prosecution was launched, allegint that Mr. Moss has committed theft of the confidential information contained in the paper. Mr. Moss was acquitted by the Liverpool Magistrate on the basis that confidential information could not be regarded as property. This conclusion was upheld by the Divisional Court, which declared that whilst the holder of infomation might possess limited rights in it which could could be upheld at Civil Law, the information itself was not a property hence could not be stolen. The editors have stated that during the parliamentary debate in England on the Theft Act it was suggested that the statutory definition of 'property' would encompass a trade secret also to enable to cover the information involved in the property. (Page 45).

The question whether temporary removal of objects will constitute a criminal offence is one which considerably predates the computer age. The issues involved are however especially relevant in this context. Given the ease and speed with which large amounts of data stored in a computer storage device may be copied, a party may obtain benefit equivalent to that normally obtained through theft by means of a temporary removal. Consideration of the situation both in Scots and English Laws have suggested different conclusions regarding the criminality of such conduct that might well be reached north and south of the border. (Page 50). Two cases which were reported in Japan are of interest and noteworthy, one of which is as follow : A computer software engineer was arrested on suspicion of stealing client information from a Tokyo Bank and selling Tokyo data base administrator. The administrator was also arrested the next day. The engineer was working free lance for Sakura Bank from where he copied the information (personal details) of 20,000 clients into a floppy disc and sold it for 200,000 yen. Yasunori Fujisama, 34 was developing client Management software for the Sakura Bank at the time of the theft. The administrator of Personal File Library, 73 year old T. Tamura, was arrested after he tried to sell the information to Sakura Bank.

In Chapter 4 (Scope of Data Protection), the editors have made it clear that there are number of ways and means by which the losses of data or information takes place and

these are mainly (i) Theft of PC and Media, (ii) Damage due to breakages, (iii) Environmental damages, (iv) Inadvert corruption/loss, (v) Environmental losses, (vi) Malicious damages/leakages, (vii) Unauthorised access, (viii) Modification Erasures etc., (ix) Computer Virus, and (x) Data Typing (Page 77) etc.

In Chapter 5, the editors have dealt with data protection principles, where it is stated that Data Protection Act establishes eight data protection principles requiring data user to ensure the following : (i) The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully. (ii) Personal data shall be held only for one or more specified and lawful purposes. (iii) Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes. (iv) Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes. (v) Personal data shall be accurate and, where necessary, kept up to data. (vi) Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. (vii) An individual shall be entitled and (viii) Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data. (Page 79). The core of the principles enumerated in this Chapter though interesting to know they were backed up with the statutory backing and in India as the computerisation is still at its primitive stage and the broad principles of data protection such as data being fairly and lawfully processed, process for limited purposes with principles of adequacy and relevancy leading to accuracy and not kept longer than the necessary time period in a secured manner and not transferred to others/other countries without adequate protection are yet to be fitted with Legal frame work/law.

In Chapter 6 (Data Protection), the Editors have rightly stated that if true progress is to be made, the task for the European Union will be to secure the minds of the third World countries persuading them of the need to introduce data protection legislation. It will only be when the subject moves beyond its Western European Kingdom and there will be the realistic prospect of control over global computer network. (Page 135).

In Chapter 7 (Information Technology and Copyright), the editors have dealt with section 79 of Information Technology Act, 2000 by referring it as Clause 78 of Information Technology Bill 1999 which speaks about liability of Internet Service Provider (ISP) and it is interesting to know about it. (Page 140 to 142). The editors have stated that the recent and controversial introduction of the Microsoft Network has prompted the adoption of an interesting legal technique by some posters to Usenet network groups. (Page 143). In Chapter 8 the editors have discussed the nature of copy right protection and before discussing the several mechanism for copyright protection the editors have discussed the rights of the copyright owner and these rights comprise (i) to copy the work or any substantial part of it (ii) to issue copy of the work to the public (iii) to perform, show or play the work in public (iv) to brought up the work or include it in a cable programme service; and (v) to make an adaptation of the work or do any of the above in relation to the adaptation. In respect of the computer programme, it is provided that adaptation means arrangement or altered version of the programme or a translation of it. The nature of copy right may include substantial similarity, literal and non-literal copying, justifiable similarities, unconscious copying, willful ignorance, acts permitted in

relation to protected work, fair dealing, error correction, back-up copies, reverse engineering and de-compilation etc. In India the Copyright Act provides protection right against any scientific or literary work. For the enforcement of violation of copyright the owner can approach local police authority for protection of right; however, the filing of First Information Report (FIR) by police authorities often takes time and it helps the pirator to destroy the evidence. In this connection the IT Act had provided adequate power to the Deputy Superintendent of Police and officers above him to act immediately to catch hold that pirator with evidence. The editors have further stated that in the eventuality of infringement of copyright being reported, the Courts are empowered to grant the reliefs such as (1) temporary and permanent injunction (2) impounding and destruction of all infringing copies, including master copies, (3) actual monetary damages + infringer's profit, (4) statutory damages, (5) court costs and reasonable fees of attorney/ s. (Page 178). The editors have stated that the laws are there, the enforcement authorities are vested with enough powers to protect Copyright. The concern is lack of awareness among citizens. Every time a consumer buys a computer loaded with unlicensed software, or buy unlicensed software product he is party to the crime. The manace of the copyright piracy or violation of Copyright effects not only the potential software development in India but also our country's economy, besides sending negative signals to potential investors. (Page 178).

In Chapter 9 (Surveillance Through Information Technology), the editors have discussed the impact of technology wherein it is stated that with the ability to digitize any form of information, boundaries between various forms of surveillance are disappearing with the application of information technology linking surveillance technique into a near seamless web of surveillance. Developments in data processing suggest that the distinction between informational and physical privacy is becoming more and more flimsy. The reach of systems of physical surveillance has been increased enormously by the involvement of the computer to digitize and process the information received. Car number plates are scanned by television cameras of the police and the details transmitted for immediate checking by computer against lists of stolen or wanted vehicles. As the net work expands it is suggested that it could become possible to find or follow almost any vehicle in Britain by tapping its registration number into a computer keyboard. (Page No. 187). While dealing with consequence of data surveillance, it is stated that as far back as 1972 in considering the threats to privacy resulting from computerised data processing, the Younger Committee identified the prospect that because the data are stored, processed and often transmitted into a form which is not directly intelligible, few people may know what is in the records or what is happening to them.

In India, the legal response to the data surveillance is growing on par with the growing international awareness, issues concerning the data, Permanent Account Number (PAN) data available with Income Tax authorities, voters identity card etc. are becoming a matter of public debate and censure as viewed by the order. (Page 193).

Chapter 10 (Individual Rights and Remedies), the authors were of the view that concept of subject access is undoubtedly the feature of data protection legislation which has the most direct impact on data subjects. Its essence is contained in the 7th data protection principles which provides that an individual shall be entitled for :

(a) At reasonable intervals and without undue delay or expense

(i) to be informed by any data user whether he holds personal data of which that individual is the subject; and

(ii) to access to any such data held by a data user; and

(b) Where appropriate, to have such data corrected or erased.

The directive also makes provision for subject access. Further there is a specific provision that Member States shall guarantee very data subject the right to obtain from the controller.

The editors have discussed the manner in which 'access right' may be exercised before attention is paid to the inevitable exceptions from access and as to the remedies which may be available to an aggrieved individual whether for breach of subject access provisions or other elements of legislation. (Page No. 194 & 195) The Law enforcement and taxation topic indicates that where data is held for the purpose of the prevention or detection of crime or an apprehension or prosecution of offenders, or the collection or assessment of any tax or duty or for any for these or more purposes, a request for access may be denied where this would prejudice the attainment of the purpose for which the data is held. The operation of this exception raises a number of significant issues. It is difficult to conceive of any item of personal data that could not be regarded as potentially relevant to the purpose of crime prevention. The exemption will apply only where the grant of access would prejudice this purpose. In the event a denial of access is challenged before the Registrar, the onus will be on the data user to demonstrate a likelihood of prejudice in the circumstances of the particular case. Whilst these issues may be susceptible of ready resolution in the contect of criminal detection and the apprehension or prosecution of offenders, some problems may be anticipated in relation to the nebulous concept of crime prevention. (Page No. 205).

In Chapter 11, the editors have discussed the E-Commerce Laws at length where the editors have discussed about the E-Commerce Laws at length.The editors have stated that the challenge for law makers has been to balance the some times conflicting goals of safeguarding electronic commerce and encouraging technological development. Ministry of Commerce initiated a draft of electronic Commerce Act and Electronic Commerce Support Act has been prepared to address the emerging issues in electronic commerce and to create a legal framework for e-commerce transaction in India. An initiative in this regard has also been taken at the level of Department of Electronics, which has drafted the Information Technology Bill which was passed on 16th May 2000, which has been recently enacted and provided as Appendices to the book. This Electronic Commerce Act aims to facilitate the developments of a secure regulatory environment of electronic commerce by providing legal infrastructure governing electronic contracting, security and integrity of electronic transactions, the use of digital signatures and other issues related to electronic commerce. The Electronic Commerce Support Act seeks to amend various central Acts (viz. Indian Penal Code, 1860, The Indian Evidence Act, 1872, the Contract Act, 1872, the Indian Telegraph Act, 1885, the Bankers' Book Evidence Act, 1891, the General Clauses Act, 1897 and the Reserve Bank of India Act, 1934 to facilitate electronic commerce. The Information Technology Act addresses the contractual issues, computer crime and data protection. It also includes a section on digital signatures.

Types of E-commerce, which include business-to-customers, (B2C) business-to-business (B2B) and customers-to-customers, (C2C) government to business (G2B) etc. The emerging concept is Government-to-Business through electronic commerce, involves electronic transaction between government and business and helps both the government and business to reduce cost and improve efficiency. Many also see electronic transaction with Government as a mean to reducing corruption and bribery. However, those countries that large in the area of electronic will find themselves at a disadvantage in attracting investment and capital. In addition to business and individual consumer the Governments are becoming a key place in electronic commerce. Governments and their citizens are also beginning to benefit from the speed, lower cost and efficiency of providing information and conducting transactions electronically. However, the real situation in South Asia except in Singapore, is that in most countries only about 1/3rd of the organisation surveyed answered 'yes' as to providing data to government electronically. Those who availed the opportunity expressed the benefits in the form of reduction of time and cost, fewer errors, quicker processing and turn around and improved efficiency. Moreover it was also noted that dealing with government electronically dramatically reduces bribery and corruption. In addition, government itself stands the benefit from the improved efficiency and lower cost of electronic transfer. Government-to-citizen electronic commerce includes filing of tax returns electronically and payment of cess, taxes, levies etc., which may take a little more time for implementation.

Issues like taxation, tariffs, data protection, authentication and copyright may require clear cut regulatory framework world-wide to facilitate e-trade. In India, the options of cyber laws and message of electronic statement of financial transaction are constrained the growth of e-business. The electronic commerce raises some new and interesting technical challenges. These include the following :

(i) Satisfying traditional legal requirements for reduction of agreement into signed document

(ii) Applying legal rules of evidence to computer-based information; and

(iii) Interpreting, adapting and complying with many other existing legal standards in the contect of electronic transactions.

From a legal prospective, one of the most significant issue in electronic commerce is how to create enforceable digial contracts for sale of goods and services or how to ensure that a digital transaction will be at least as enforceable and valid as a traditional paper based transaction. In every business environment whether the transactions are executed in person (face to face) or overdistance, there are accepted customs and practices that determine, in conjunction with applicable legal rules, the parties, rights and responsibilities. These practices often include controls, such as signatures to evidence agreement, time and date — stamping to provide proof of despatch submission, receipt or acceptance and in some cases witness, notaries and other trusted third parties to acknowledge and authenticate a transaction.

The Information Technology Act, 2000 recognises digital signatures India and enable for its use. It has defined digital signature and provides for the use of digital signature to authentic an electronic record (Electronic Record means data record or data generated,

image or sound stored, received and sent in an electronic form). In the buzz of E-Commerce today, another killer ‘app’ on the internet — E-mail should also use digital signature to authenticate communication was the view expressed by the authors.

In the 12th Chapter, the author has discussed about Cyber Crime and the Law. Different types of Cyber Crime such as (i) Phveakers; (ii) Fraud; (iii) Hackers; (iv) Pronography; (v) Viruses; (vi) Pedophiles; (vii) Harassment; (viii) E-mail security destruction; (ix) Data didding (x) Violation of privacy; and (xi) Crackers etc. To prevent the cyber crime various safety related issues are available at the site indicated below :

(i) Child safety on the internet

(ii) Computer Crime Resources

(iii) Cyber Patrol

(iv) Cyber Sitter Product Info

(v) Keeping Kids safe in cyberspace

(vi) Safe Surf home page

(vii) Safe Surf back issues

(viii) Safe Suft Inc.

(ix) Street smart on the web

(x) Surf watch Home page.

Overall, the book provides valuable information and case law. Various issues relating to data protection are dealt by the editors in a systematic way. Readers will find that the Info-tech legal aspects and the western experience in handling the e-commerce problems and connected legal issues relating to globalisation of e-business etc. really provide a good insight. In short, the book is definitely worth its price.