International Journal of Academic Research
ISSN: 2348-7666; Vol.4, Issue-1(1), January, 2017
Impact Factor: 4.535; Email: drtvramana@yahoo.co.in

Critical Study on Cyber Laws Related to Information Technology Act - 2000

M.Narsingh, M.A.LL.M (Corporate Laws), University College of Law,
Osmania University, Hyderabad, Telangana State, India.

Abstract: The cyber world has no physical boundaries, no single authority who governs the internet. The internet is the medium for freely sharing information and opinions; it provides everyone with round the clock access to information, credit and financial services, and shopping. Even network information systems are being adopted by the governments worldwide, that is why the governments across the world are recognizing the need to securing and regulating the cyber world. Cybercrimes are a new class of crimes which are rapidly expanding due to extensive use of internet.
Key words: Cybercrimes, technology, Human history

Introduction:

Human history in a sense is a story of technology from flint stones to that of genetic clones. The tribulations and triumph of such a journey, which will continue in the future, has one aspect, constant at its core – "the law that governs them". Technology – if defined as 'set of refined processes resulting in various application of daily use in our lives' seems to be harmless marvel in its basic construct and explanation. A deeper understanding and implications of 'technology' could lead us to other scary construct. Leading such a thought is the 'nuclear technology' perfected to the core and yet a debate on how to 'deconstruct' the same. Hence, the inevitable intervention of 'law' on shaping , banning and encouraging ' technology' remains a constant. 'Law' as an instrument of 'governance of human behaviour' closely shadows 'technology'. According to Harold A.Linstonem, - The pace of growth of technology and governance are not compatible raising a series of serious problems. The combination of explosive population growth and rapidly evolving technology is in effect shrinking the earth to a global village. The earth's 5.77 billion in 1996 may swell to 9.4 billon by 2050.

At the same time the widening gap between technological and organizational rates of change is producing a growth mismatch: we are approaching the new era with 21st century technologies, 20th century governance process and 19th century governance structures. Some view this mismatch as one between physical and social technologies. The combination of shortsightedness, irresponsibility, gullibility, human greed, and fear of change is impending homeostatic evolution of a knowledge society. Demographics are playing a significant role in the widening gap in the developed world. Youth have galvanized the information technology revolution: the personal computer or PC is the creation of starting young computer hackers and entrepreneurs (e.g. Steve Jobs of Apple and Bill Gates of Microsoft).

The urge to minimize the yawning technology – organization chasm suggests two possibilities:
Path 1 – Slowing down the technological pace of change, this scenario is unthinkable for most people, particularly scientists and engineers. The technological pace appears unstoppable. A new Dark Age is as inconceivable as it must have seemed to the forecastses in the Golden Age of Imperial Rome.

Path 2 – Accelerating the organizational pace of change – there is little question that information, communication and transportation technologies permit dramatic and profound changes in organizations and governance. Industry is already showing us new forms of organization such as downsized, "virtual", decentralized and global corporations. Taking just one example, we see today that Information Technology makes possible as never before simultaneous localization and globalization, fragmentation and integration, decentralization and centralization, in many societal aspects. Organizational innovation based on coordination – intensive structures is one consequence.

The term 'Cyber Space' was coined by Novelist William Gibson, denotes a place without physical walls or even physical dimensions which has connected to globe in the shortest span of time to the extent no technology has done before in human history. Cyber law means law of the Internet, law relating to computers or law governing cyberspace. Cyber laws is an evolving one which interfaces with all the constitutional provisions, various statutes of other traditional branches of law, various other cases involving individuals, corporate and institutions who transact through the 'Internet' using the emerging technology of hardware and software. Such a sketch will include interfacing technology processes like telecom, Internet services, educational services, cable and broadcasting services, media services, regulatory services, law and order agencies, intelligence services, entertainment services, health services, financial services, judicial services and others which may become part of this future revolution. In short it encompasses all services and players of such services who use and consume 'internet'.

Cyber law governs the legal issues of cyberspace. It comprises the following issues:

1. Cyber Contracts
2. E-Commerce
3. Digital Signatures
4. Intellectual Property Rights
5. E-Governance
6. Cyber Crimes
7. Data Protection & Privacy

The cyber world has no physical boundaries, no single authority who governs the internet. The internet is the medium for freely sharing information and opinions; it provides everyone with round the clock access to information, credit and financial services, and shopping. Even network information systems are being adopted by the governments worldwide, that is why the governments across the world are recognizing the need to securing and regulating the cyber world. Cyber crimes are a new class of crimes which are rapidly expanding due to extensive use of internet.

The Information Technology Act, 2000 is a step in this direction. It is with this aim that this Act was enacted to secure a regulatory environment for e-commerce by providing a legal framework governing e-contracting, security and integrity of e-transactions, use of digital signatures and other connected issues. Electronic trading, the formation of contracts for the provision of goods and services, payments under such contracts and the transfer of property are all being transacted through the process of electronic data interchange. There are a number of legal issues which this system presents. These may include, the requirement of writing; the requirement of a document; the requirement or signature; the requirement of an original; and risk allocation.

As the law moves to catch up with development, information technology moves at a much faster pace, creating a void between the two. Legal issues relating to Internet and e-commerce hinge on the issue of jurisdiction of courts, In a particular case in question. Jurisdiction is the most problematic legal issue in e-commerce.

The problems can be numerous, and the solutions are to be found for them. The scope and extent of law is more important, in view of the geographical differences of contracting parties. To confront effectively the emerging problems, in addition to enactment of a suitable law, the existing laws have to be attuned and amendment to meet the need of changed circumstances.
The United Nations Commission on International Trade Law (UNCITRAL) adopted, in June 1996, a Model Law on e-commerce, intended to give States a legislative framework to remove barriers of e-commerce. The Model Law provides, among other things, that where the law is requires a signature, it could be met electronically if e-signature provided a link between the signer and the record and evidence of intent to be associated with the record, both to be sufficiently reliable for the purposes of the record.

The Information Technology Act, 2000 was based on -the UNCITRAL Model Law, which facilitates the regulatory mechanism in respect of the issues relating thereto. This step by India to enact this legislation is a timely one and would help in dealing with issues relating to cyber space. The corresponding amendments in other legislations are in tune with the provisions of this Act are also a welcome step for realization of the objectives of the Information Technology Act, 2000.

Information is data put into a meaningful and useful context. A society where information, rather, material, machine or energy is the dominant technology is known as an information society. This is why computers play the most important role in our day-to-day life. The first computer ever developed was in the year 1946 and was known as the Electronic Numerical Integrator and Calculator. We are in the Fifth Generation of computers now. As far back as 1994 it was estimated that around two-thirds the developed world's economy would be reliant on some form of information technology.

The kinds of functions these computers perform are astounding to say the least.

They store and process large volumes of personal information of great importance to the users. This information stored in the computers becomes the property of the user. This kind of property needs protection from people trying to appropriate it. There are a number of ways in which this can be done like unauthorized access, computer viruses, data typing, modification erasures etc. and all these caused great public concern. The 1960's saw the emergence of Privacy as a value that could not be taken or misused by government without due process of law. Legal protection of an individual's privacy can be described as capricious and sporadic. Where it exists at all, it comes from a diverse variety of sources, such as the law of breach of confidence, the torts of defamation and malicious falsehood and, to some extent, indirectly through copyright. Of course, the perennial difficulty for legislators is balancing the rights of individuals with freedom of expression: an almost impossible task.

The concept of Data Protection brings in a paradox on the one hand Data Protection seeks to give an individual a greater measure of control over personal information and to place control over dissemination of information and on the other it conflicts with another individuals claim to be allowed access to information under basic human rights.

This led to a debate centered on private data. It was this informational aspect of privacy that was most profoundly affected by the rapid developments in information technology during the 1960's. Concerns about the increased use of the computer and the setting up of national databanks were growing. In these circumstances, the choice of the individual was seen as central to the concept of privacy of two kinds viz. allowing physical intrusion and the sharing of information.

Thus, it was in the year 1970 that the first computer specific statute was enacted in Germany in the form of a Data Protection Act. The concept of Data Protection is one of the most significant contributions to the law of information technology. This statute of the Germans was widely accepted all over Europe and throughout much of the world.

II. Origin of Data Protection Laws in the UK

In the UK, a committee on Privacy was setup in the year 1972. A report submitted by this committee formed the basis for the enactment. During that time the dangers were still potential and not real.

The Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data was an attempt to impose a regime on the processing of computer data relating to individuals such that the risks to privacy and freedom would not be unduly compromised. The Data Protection Act 1984 was the United Kingdom's response to the Convention and can best be described as taking a minimalist approach. Compliance with the 1984 Act has been seen as little more than a regulatory chore and the Act has done little to consolidate and enforce individuals' rights and freedoms in respect of personal data relating to them. Although individuals were given

rights of access to their personal data and rights to compensation in certain circumstances, most persons who felt aggrieved complained to the Data Protection Registrar who could then exercise the powers of investigation and enforcement.

The 1995 European Union (EU) directive relating to data protection and the subsequent introduction into the UK of the Data Protection Act 1998 (DPA) together with the incorporation of the European Convention of Human Rights (ECHR) into UK law with the Human Rights Act 1998 (HRA) has seen a much wanted change in the law of privacy. The Data Protection Act 1998 attempts to address and reconcile the tensions between rights to privacy and the goals pursued by persons processing personal data.

The Data Protection Act establishes eight data protection principles requiring data users to ensure that:

(1) Personal data shall she obtained and processed fairly and lawfully.
(2) Personal data shall be held only for one or more specified and lawful purpose.
(3) Personal data held shall not be disclosed.

(4) Personal data held should not be more than what is necessary for the purpose for which it has been collected in other words it should be adequate.
(5) Personal data shall be accurate and up to date.

(6) Personal data shall not be stored for longer than it is required.

(7) Appropriate security measures shall be taken against unauthorized access to or alteration of personal data.
(8) An individual shall be entitled.

The Data protection Act provides for some exemptions Le., information that can or shall be disclosed as the case may be. Information, which is required by law to be made available to the public, shall be disclosed e.g. electoral roll, Payroll and Accounting Data so long as the data is not used for any other purpose, e.g., using credit card numbers. Mailing lists, data of unincorporated members clubs, data held for management of personal or family work where all those whose details are held have consented for processing. The Data Protection Act 1998 has failed to make a significant contribution to privacy rights in the UK. While the Directive aimed to protect privacy, there is no mention of the word 'privacy' in the UK Data Protection Act 1998. Further, as seen earlier, transparency in the processing of data had been compromised by various exemptions from subject information provisions and, in many cases, from the requirement to notify the Commissioner of processing of personal data. The 1998 Act is based on the European Convention, about 2 decades old now. The data protection principles contained within it are a reflection of what is now incredibly dated technology. Current computer technology is light years ahead of what was around in the early 1980s and of particular importance is the phenomenal growth of global networks such as the Internet.

III. India and data protection laws

In today's world, the greater use of information technology coupled with the growing reliance on data and new

and sophisticated uses of it make it imperative to have an effective yet workable data protection law. Surprisingly, India does not have one. Except for section 72 of the Information Technology Act, 2000 which talks about 'Breach of Confidentiality and Privacy' and Section 43 which talks about 'Penalty for damage to computer, computer system etc,' no other section or Act talks about Data Protection. The implications of not having such a law are many.

Lack of computer privacy legislations may affect India's overseas trade. It becomes extremely difficult for the multinational enterprises to comply with different standards of data protection, in every country in which they have acquired, stored, processed and transferred data. In the age of Internet, where all information is transferred through 'cyberspace' India could well become a "pirate offshore data haven" i.e. where a country wants to protect its citizens liberties by placing restrictions upon the forms of data processing, this step could be easily nullified by transferring the data elsewhere, where there are no such laws for processing.

India can rely on the British experience greater weight has to be given to the principle of transparency. It has to be made the central plank of the new law. There should be no compromise in this matter. Transparency in this context would mean letting the person whose data is being accessed know about it. As under the 1984 Act, individuals have a right to be informed as to whether the data controller is processing data concerning the particular individual and, if so, a right of access to that data. The Data Protection Directive goes further in requiring the provision of additional information such as the purposes of the processing. This has to be incorporated. Some of the cumbersome provisions relating to data subjects and automated decision taking can be done away with. India needs to have such a legislation. Right to Privacy is not a fundamental right in India. It can be read into Article 21 of the Constitution. When the Data Protection Bill is made this has to be kept in mind.

With the recent trends showing an increase in Internet and information technology related crimes the time has come for India to enact a legislation to protect the transfer of information.

The foregoing analysis clearly brings out the importance of application of cyber technology. Today crimes are been committed on an increasing scale even in the field of cyber law. There is every need to you all important principles for protection of data in the field of internet and information technology the topic is of great contemporary importance and accordingly it has been selected as the subject matter of the present dissertation.

a) Area of Research

The following matters are critically examined in the present thesis.

1. Importance of cyber Law.
2. Crimes under Cyber law.
3. Need for data protection under Cyber Law.

b) Hypothesis: Greater weight has to be given to the principle of transparency. It has to be made the

central plank of the new law. There should be no compromise in this matter. Transparency in this context would mean letting the person whose data is being accessed know about it. As under the 1984 Act, individuals have a right to be informed as to whether the data controller is processing data concerning the particular individual and, if so, a right of access to that data. The Data Protection Directive goes further in requiring the provision of additional information such as the purposes of the processing. This has to be incorporated. Some of the cumbersome provisions relating to data subjects and automated decision taking can be done away with. India needs to have such legislation. Right to Privacy is not a fundamental right in India. It can be read into Article 21 of the Constitution. When the Data Protection Bill is made this has to be kept in mind. With the recent trends showing an increase in Internet and information technology related crimes the time has come for India to enact a legislation to protect the transfer of information.

c) Methodology followed: There are different types of .Methods that can be adopted in the preparation of thesis. These methods are broadly divided into 2 categories a) Traditional b) Scientific The traditional methods are – (i) Philosophical (ii) Institutional (iii) Legal (iv) Historical The scientific methods adopt an empirical approach ie., an analysis of facts based upon the evidence of existing facts and material. In the preparation of present thesis both kinds of approaches have been adopted. Thus a historical cum analytical approach has been followed in the preparation of present thesis. Where required the comparative approach has also been adopted to bring about the clear meaning of the provisions of the act by comparing them with similar provisions under other systems.

d) Sources of Information: The information for the thesis can be collected by following any of the two approaches – (a) A doctrinal approach; (b) A non-doctrinal approach. Doctrinal approach is also known as fundamental approach. It is also described as textual in nature. It consists of 2 kinds of sources - (a) Primary (b) Secondary . The primary sources are concerned with legislation and case law. The secondary sources are concerned with articles published in leading journals, law reviews text books etc. The non-doctrinal approach is known as functional or contextual. It deals with social values, constitutional interrelations, principles of justice, good conscience etc. In the preparation of the present thesis mainly the doctrinal approach has been adopted and the necessary material equity has been drawn from both primary and secondary sources.

Conclusion & Suggestions: The major issues in the Cyber Contract are the technical issues relating the authenticity of the electronic record, the receipt and acknowledgement of the record, the time and place of the concluding of the contract. Based on these issues only, the jurisdiction, application laws are decided. The Information Technology Act, 2000 has been incorporated to resolve these technical issues, and the Information Technology Amendment Act, 200 has brought vital changes to the act and increased its application and scope. But

in practical scenario, in comparison to the laws of United States and European Nations, there is still a lacuna and more development and improvement shall be made in the administrative mechanism for the implementation of the laws. There is urgent necessity to educate the judges, police and enforcement mechanism about the vital importance of the cyber transactions and increase the efficiency of the same. It is a known maxim that "Prevention is better than cure", as such, it will be more effective and productive if the rules and regulations are of preventive nature i.e. norms and regulations can be brought, making it compulsory for the parties to follow the set of rules to enter into contract. Even awareness shall be brought in the public-at-large, relating to the ever growing circumference of the Cyber Contracts. However, it is past time to develop common standards for E-Commerce throughout the globe. Not only should jurisdictional outcomes be as predictable as possible, they should be as uniform as possible.

References

Praga Diwan: Cyber and E-Commerce Laws, 2nd edn, 2000, Bharat Publishing House, New Delhi
K.Mani: A Practical Approach to Cyber Laws, The IT Act, 2000, Kamal Publishers, New Delhi
Nitant P.Trilokekar: IT Act, 2000, 1st edn, 2000 Snow White Publications, New Delhi
The IT Act, 2000, Bare Act, Kamal Publishers, New Delhi
SB Sinha: Cyber Crime in the Information Age
Farooq Ahmed: Misapplication of Uniform Domain Name Dispute Resolution Policy
Aarti Dubey: Cyber Law and Terrorism
Subhash Gupta: IT Act, 2000 and its drawbacks
Narahari Lenka: IT Law and policy
G.Aruna Kanthi: Money in electronic age
G.Rajasekar Rohan George: Illegal activities on the internet
Chetana RG: Combating obscenity on the internet
Web sites: www.indlii.org, www.alertindian.com/node/5 , www.cyberlawsindia.net

Recent Articles and Journals