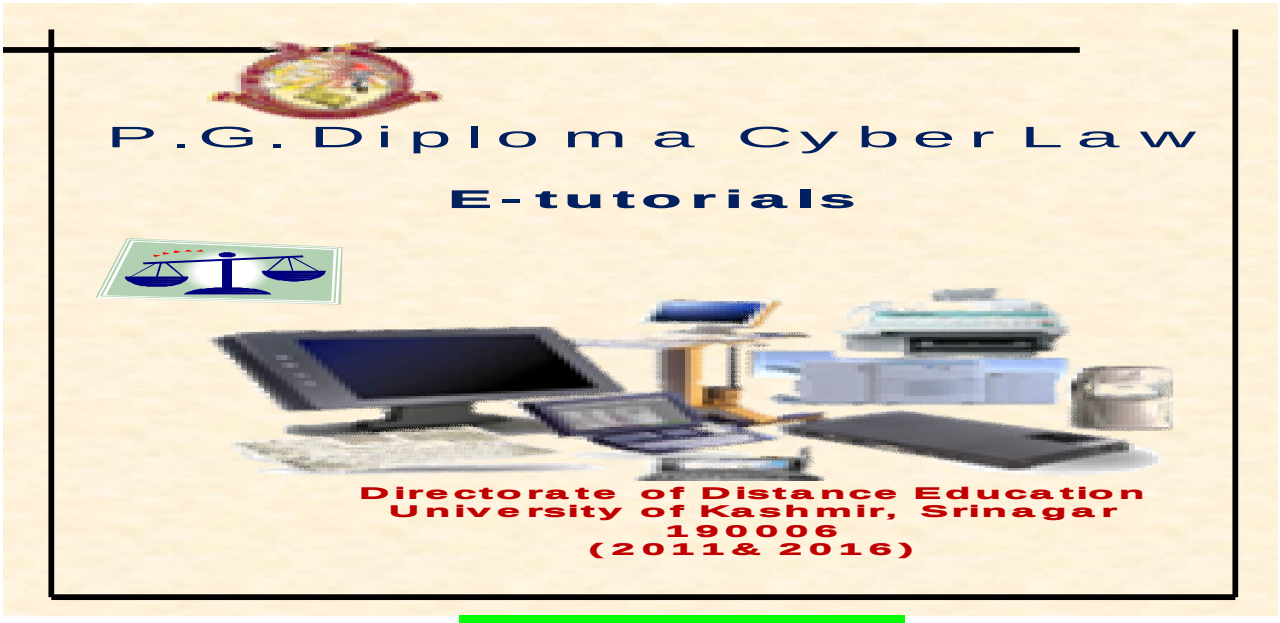

E-TUTORIAL NO.1-3

SUPPLIMENTARY

Prepared by:
Mushtaq Ahmad(NET,LL.M;Ph.D)
Associate Professor(Law Courses)
Directorate of Distance Education
University of Kashmir(2011& 2016)

Published by:
Directorate of Distance Education
University of Kashmir

Year of Publication:*2011(print),*
e-tutorials 2016

E-tutorial No:1-3

An Overview of Cyber Law

(Information Technology Act, 2000
&)
Information Technology (Amendment) Act, 2008)

-

1 Laws to Regulate Conduct in Cyberspace

The use of information communication technologies has opened new opportunities, enhanced government services to the citizens, increased citizens participation in policy making and development. The millions of people can be benefited by the use of technology, the government and business enterprises can play an important role in promoting the use of technology. Today we talk of information technology, information society. With the development of networks which has provided global access and sharing of information among the computer users, the explosive growth can be seen in a virtual medium called cyberspace, the commerce is growing in cyberspace especially as methods have been developed to make credit card transactions reasonably safe (Rupley 1996). However this new mode of transaction has raised several concerns for regulation, to develop guidelines in relation to consumer protection issues, to impose criminal penalties for computer and cyber crimes. The biggest challenge is the making of technology based law. The Cyber Laws should also include the whole sets of legislation that can be applied on the transactions taking place through internet. This unit gives an overview, Genesis, scope and object of the Information technology laws in India, the Information technology Act and how the current version of Information Technology 2008 has been evolved.

The first technology based law in India was the telegraph Act, 1885. This law was framed with the advent of telegraph and later it also covered the telephone. The information Technology Act, 2000 (IT Act 2000) is the most significant Act which accords legal recognition to electronic records, digital signatures and impose penalties for various cyber offences. However apart of Information Technology Act there are many other acts that can be applied to govern and regulate conduct in cyberspace. For determining the legality of online contract act the provisions of Indian Contract Act, Sales of Goods Act 1930, can be resorted to. To curb the violation of the use of online

sources of information, the Copyright act, Trademarks Act can be used. To provide relief to the online consumers, the following different acts like the Consumer Protection Act, the Competition Act 2002, companies Act, the Banking Regulation Act, Securities and Exchange board of India Act, Cinematograph Act 1952 can also be applied.

The United Nations General Assembly with the aim to promote standardisation and homogenisation of International laws by resolution A/RES/51/162, dated the 30 January 1997 adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law referred to as the UNCITRAL Model Law on E-Commerce. This model law establishes rules and norms that validate and recognize contracts formed through electronic means, lays down rules for contract formation and governance of electronic contract performance, defines the characteristics of a valid electronic writing and an original document provides for the acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence in courts and arbitration proceedings. India is a signatory to the Model Law. Following the UN Resolution India passed the Information Technology Act 2000. It is an Act of the Indian Parliament (No 21 of 2000) as notified on October 17, 2000. The Electronic Transactions Act 1998 of Singapore also significantly guided the framing of the Act.

1.1Objectives of the Act-

The main objective was to regulate the use of computers, computer systems and computer networks as also data and information in the electronic format. The Preamble to the Act states that it aims at providing legal recognition for transactions carried out by means of electronic data interchange and other means of

electronic communication, commonly referred to as "electronic commerce", which involve the use of

alternatives to paper-based methods of communication and storage of information and aims at facilitating

electronic filing of documents with the Government agencies.

The Act was enacted with a view to give a fillip to the growth of electronic based transactions, to

provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer

based crimes and ensure security practices and procedures in the context of widest possible use of

information technology worldwide. The information technology act seeks to protect the advancement in

technology by defining crimes, prescribing punishments, laying down procedures for investigation and

forming regulatory authorities. The act not only lays down new substantive law but also makes incidental

and consequential amendments to other laws, many electronic crimes have been bought within the definition

of traditional crimes too by means of amendment to the Indian Penal Code, 1860. The evidence act, 1872

and the Banker's Book evidence act 1891, and reserve bank of India act, 1934 have been suitably amended.

1.2 Applicability of the Act

The Act extends to the whole of India. S. 1(2) provides that it shall extend to the whole of India and,

save as

otherwise provided in this Act, it applies also to any offence or contravention there under committed outside

India by any person. However as per section 75(2) it will apply only if the act or conduct constituting the

offence or contravention *involves* a computer, computer system or computer network in India. Section 81

provides effect to the provisions of the Act notwithstanding anything inconsistent contained in any other

law for the time being in force. The list of excluded documents (to which the Act will not apply) as

provided in Section 1(4) has been removed by amendment and a notification through Gazette is required

for excluding any document from the Act. Schedule I of the new Act contains the list of excluded documents

as per the earlier Section 1(4) and that can be considered as meeting the requirement of the notification at

this point of time. The excluded Documents are: a Negotiable instrument; power of attorney; trust; a will;

any contract for sale or conveyance of immovable property or any interest in such property.

2 Salient Features of the Information Technology Act

- The Act has adopted a 'functional equivalents' approach whereby paper-based requirements such as
  record, document, signature etc are replaced with their electronic counterparts.
- It extends to the whole of India (Section 1) and specifically prohibits the application in certain situations.

- It applies also to any offence or contravention there under committed outside India by any person. section 75

  (1) provides that the Act is also applicable to any offence or contravention committed outside India by

  any person irrespective of his nationality, however, an exception to this rule has been laid down in Sub

  section (2) which states that for the purposes of sub-section (1), this Act shall apply to an offence or

  contravention committed outside India by any person, if the act or conduct constituting the offence or

  contravention involves a computer, computer system or computer network in India. In effect, if an act

  (amounting to an offence under the Act) has been committed and where any computer, computer system

  or computers which are interconnected to each other in a computer network and which is in India is also

  involved (which might be either as a tool for committing the crime or as a target to the crime), then the

  provisions of the Act would apply to such an act. Section 81 of the Act further provides that the provisions

  of the Act shall have effect not withstanding anything inconsistent therewith contained in

  any other law for the time being in force.
- The act provides for the legality of the electronic format i.e., electronic documents, electronic contracts.
- Chapters III deals with electronic Governance and chapter IV is exclusively on electronic records.
- The act deals with various aspects pertaining electronic authentication (sec-3); legal recognition of electronic

  records (sec 4); retention of electronic records (Sec 7).

- It provides legal recognition to Digital Signatures (Section 5). Digital Signature has been vastly covered

  under Chapters II, VI, VII and VIII of the act. Section 3of the act provides Legal Framework for affixing

- Digital signature by use of asymmetric crypto system and hash function which envelop and transform the

  initial electronic record in to another record.

- Section 8 of the Act provides for Publication of rules, regulation, etc., in Official Gazette or in electronic

  form in electronic Gazette.

- The concept of secure electronic records and secure digital signatures and the security procedure has been

  dealt in Chapter V of the act (see Sections 14, 15and 16 of the act).

- Provides for licensing and Regulation of Certifying authorities for issuing digital signature certificates

(Sections 17-42).

- Section 18 deals with Functions of Controller. Section 19 deals with recognition of foreign Certifying

  Authority as Certifying Authority for the purpose of this Act.The Controller shall act as repository of

  all digital signature certificates. (Section 20)

- The Various types of Offences and stringent penalties under the Act have been enumerated in Chapters IX

  and XI of the act. (Section 43 and Sections 66, 67, 72).

- Sections 43 deals with penalty for damage to computer, computer system. (damages by way of compensation

  is to be paid to the person so affected ,not exceeding one crore rupees).

- Sections 46 & 47 of the act provides for appointment of adjudicating officer for holding inquiries.

- Sections 48-56 of the act (Chapter X) provides for establishment of the Cyber Regulations Appellate

  Tribunal.

- Appeal from order of Adjudicating Officer lies to Cyber Appellate Tribunal and not to any Civil Court

  (Section 57).Appeal from order of Cyber Appellate Tribunal lies to High Court (Section 62)

- Section 70 provides that government by notification in official gazette declare any computer, computer

  system or computer network as the Protected System

- The Act also applies to offences or contraventions committed outside India (Section 75).Investigation

  of computer crimes to be investigated by officer by the Deputy Superintendent of Police (DSP)(section 78).

- Chapter XII deals with the issue of liability of network service providers. In certain cases they are also

  exempted from liability (see Section 79).

- There is provision that police officers and other officers have Power to enter into any public place and

  search and arrest without warrant (Section 80)

- Offences by the Companies (Section 85)

- Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and

  Controller (Section 88).

- Chapter XIII deals with residuary matters like police powers, removal of difficulties, power to make

  rules and regulations, amendment to various enactments, etc.

- There are four Schedules to the Act each dealing with amendments to the four enactments as

given below:

- The first schedule- amendments to the Indian Penal Code, 1860.
- The second schedule- amendments to the Indian Evidence Act, 1872.
- The third schedule- amendments to the Bankers Books Evidence Act, 1892.
- The fourth schedule- amendments to the Reserve Bank of India Act, 1934.

- Under the Act, following rules, regulations and guidelines have been framed:

(a) the Information Technology (Certifying Authorities) Rules, 2000;
(b) the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000;
(c) the Information Technology (Certifying Authority) Regulations, 2001and;
(d) the Guidelines for Submission of Application for Certifying Authority, 2001.

3 Criticism of the Act and Need for Amendment.

In the era of new technology and the global sharing of information and development of e-markets,
the IT Act, 2000 was the much needed cyber-specific legislation for regulating activities taking place
through cyberspace. Though there are many advantages of the Act, there are still some anomalies which
can be improved upon.

There has been a general criticism of the wide powers given to the police under the Act. It has been

labeled as draconian as the provision in Section 80 of the Act enables the Police to "Arrest a person without

warrant". The Police and other central government officials have been given arbitrary power that they can

enter and search without any warrant with the purpose to prevent any cyber crime, any public place which

includes any shop, public conveyance, hotel or any place accessible to and be used by public. The Central

Government and its officials, including the police, have been also given immunity from any suit,

prosecution and other legal proceedings for any act, done in good faith, in pursuance of the provisions of the

Act. This rule out the remedy for any person, who is made a target of abuse and misuse of the power by the

police. In the democratic era, this not only invades the privacy of the person accused but also violates

his right to live with dignity and therefore there is need to enquire and evolve a balanced solution.

Further, it is not clear which offences are cognizable or bailable under Information Technology Act,

2000. At the same time some complaints on Internet Leeching and Phishing were refused to be registered

under ITA 2000. There were several instances when employees of a firm were arrested under Section 66

based on the complaint made by the disgruntled employer. The Police used their powers or have refused

to use their powers on considerations other than what ITA 2000 prescribed. No Court or Human Rights

Commission was called upon to take a view on these issues also (*see Naavi.org, Is ITA 2000 Stringent*

Enough on Cyber Criminals?)

The Information Technology Act, 2000 did not provide for adequate Data protection

provisions. The act does not have specific provision to deal with crimes relating to domain name disputes,

identity theft, Impersonation, cyber stalking, cyber defamation, and Cyber Terrorism. The act is also

silent on privacy related issues, and did not contain any provision for providing lawful safeguards to

protect liberties of citizens.

As the technology is constantly changing, there is a criticism that the Act binds digital signatures to the asymmetric encryption system thereby limiting the scope of innovation in technology. A single section devoted to liability of the Network Service Provider is highly inadequate. The issues are many more. Under the Act liability of the Network Service Providers is restricted only to the Act or rules or regulations made there under though the service Providers liability can also be fixed under other enactments like the Copyright Act or the Trademark Act which is not clarified. However the actual implementation and the interpretation of the various provisions of the Act by the judiciary and the existing flaws in it will be tested only in the long run.