
UNIT 1 DOMESTIC LAWS: BACKGROUND

Structure

- 1.1 Introduction
- 1.2 Objectives
- 1.3 Challenges to Laws
- 1.4 Information Technology Act, 2000
 - 1.4.1 A Quick Overview of the Act
- 1.5 Critiques of the I.T. Act
- 1.6 Proposed Amendments to the I.T. Act
- 1.7 Summary
- 1.8 Terminal Questions
- 1.9 Answers and Hints
- 1.10 References and Suggested Readings

1.1 INTRODUCTION

This is the first unit of the first block of Course 2. This unit discusses the main challenges posed by information and communication technology to the law. This unit also gives an overview of the IT Act, 2000 and discusses the amendments suggested by the expert committee set up by the government.

The phenomenal growth of Information and Communication Technology has in a span of a few years significantly changed our way of life. It has changed the way of business, governance, communication, education, entertainment almost every conceivable activity in society. Computers and internet connectivity along with the phenomenal advance in telephony have been the foundation of this revolution.

We are now in the age of the information society wherein it is recognised that “information and communication are at the core of human progress. Rapid progress of these technologies opens completely new opportunities to attain higher levels of development.”(From the Declaration of Principles, World Summit on the Information society, ‘Geneva 2003 and Tunis 2005). It has been realised that this technology can in benefit millions of people and therefore governments as well as other stake holders have a key role in promoting the spread of the use of the technology more so with the intent to bridge the digital divide that represents the uneven distribution of the benefits of information technology today.

India today is emerging as a global information technology powerhouse, offering high quality IT and IT enabled services at low cost and therefore the IT sector is of immense importance and of great priority for the government. The sector is witnessing rapid growth with exports to the tune of Rs. 78,230 crores in 2004-5. This growth also has a significant effect on the Indian economy. This sector has also risen to become the biggest employment generator in the

country, the number rising from 2.8 lakhs in 1999-2000 to 10 lakhs in 2004-05. Apart from the direct impact on national income and employment, the IT sector has contributed to the growth of several ancillary businesses such as transportation, catering etc. The country has also witnessed a real estate boom stemming from the boom in the IT sector.

The phenomenal connectivity of the net has logically led it to become the most potential instrument for economic activity and governance; **e-commerce** and **e-governance**. With the development of this new technology, and with the realisation that such technology affects human life and relations, societal peace and order and proprietary rights, it was felt that there was a need for laws to regulate conduct in cyberspace accordingly. The need to regulate was also felt because of the immense potential that the medium has to contribute towards development, which can be achieved only through an optimum policy and legal regime governing it. Thus the Internet which as a medium has had a *laissez faire* growth with 'netizens' all over the globe voluntarily contributing substantially to its expansion is now coming more and more within the ambit of governmental regulation. Regulations relating to the Internet are being made today by national government and also by international intergovernmental bodies and international organizations. The whole body of laws and regulations both national and international governing cyberspace constitutes what is known as cyber laws. This however does not mean that the cyberspace does not continue to be an area of expression and innovation for adventurers. Almost on a daily basis human innovation and expression is visible on the Internet.

While going through this and subsequent 2 units, it is recommended that you should keep a copy of the IT Act with you because on many occasions you would find it beneficial to read the sections and subsections of the Act relevant to the topic you are studying.

1.2 OBJECTIVES

After studying this unit you should be able to:

- discuss the challenges which the law should address to keep pace with the new information and communication technology;
- describe the legislative measures taken by India to address the challenges;
- examine as to what extent the IT Act has been able to address the challenges posed by the information and communication technology; and
- discuss the amendments as suggested by experts to make the more effective Act in regulating the area.

1.3 CHALLENGES TO LAWS

The biggest challenge to the law is to keep pace with technology. While talking about crimes relating to the Internet, most traditional crimes like fraud, defamation committed while using the Internet etc, would be governed by the existing technology neutral criminal laws. These are crimes with all elements of offline crimes, the only difference being that the Internet was used as an aid in their commission.

The second kind of crime is the one directed at computers, networks, data etc. These are the crimes that need to be newly defined and prohibited for the purpose of maintenance of order. They include unauthorized disruption of computers and networks, the heart of what most people consider cyber crime. It occurs when an entity, without permission, interferes with the functionality of computer software or hardware. They are more familiar as viruses, worms, logic bombs, Trojan horses, and denial-of-service attacks. Unauthorized access to computer programs and files and theft of identity are the other categories of offences directed at computers.

Some of the challenges of making technology based laws are that there is a chance of them being soon outdated. Therefore, it is desirable that laws as far as possible must be drafted in a technology neutral way. Again it is against equity and fairness if offline conduct is governed differently from online conduct. This give rise to the possibility of crime shifting from one place to the other if there is an inconsistency in laws. Consistency between the two laws is therefore desirable. Laws must also cater to the need of prevention and investigation of crimes. For instance, with the advent of telephones, wire tapping laws were introduced, similar laws to deal with unlawful conduct in the Internet would become necessary.

The first technology based law in India was the Indian Telegraph Act of 1885. This law was framed with the advent of the telegraph and later covered yet another advance in technology, the telephone. In the domain of technology driven law falls the Information Technology Act, 2000. While the Information Technology Act is the most significant Act addressing conduct in cyberspace in India, there are a whole lot of other Acts that would apply to govern and regulate conduct and transactions in cyberspace. Take for instance online contracts. Apart from the relevant provisions of the IT Act like Sections 12 and 13, the Indian Contract Act, the Sale of Goods Act, 1930 etc would be relevant to determine the legality of such contracts. Further the provisions of the Competition Act, 2002 or in case of unfair trade practices, the Consumer Protection Act 1986, would also be relevant.

Protection of intellectual property available on the Internet is one of the greatest challenges of the day. Be it books, films, music, computer software, inventions, formulas, recipes, everything is available on the net. Protection of copyrights trademarks online would entail the invocation of the Indian Copyright Act and, the Trade Marks Act.

As far as illegal activities on the net are concerned, apart from specific provisions in the IT Act that penalizes them, a whole gamut of other Acts would govern them. For instance in case of an Internet fraud, based on the nature of the fraud perpetrated, Acts such as the Companies Act, 1956, the Securities and Exchange Board of India Act, the Banking Regulation Act, the Public Gambling Act, 1867 and the Indian Penal Code would also apply. For online pornography while section 67 of the IT Act would apply, section 293-294 of the IPC as well as the Cinematograph Act, 1952, the Indecent Representation of women Act and the Young Persons (Harmful Publications) Act, 1956 would apply. For matters relating to Internet sale of prohibited

substances like arms and narcotics the Arms Act, 1959, the Explosives Act, 1884, the Narcotic Drugs and Psychotropic substances Act, 1985 would apply.

Thus it can be inferred that while the IT Act is the quintessential Act regulating conduct on the Internet based on the facts of a case or the nature of a transaction, several other Acts may be applicable. Therefore, cyber laws includes the whole set of legislation that can be applied to determine conduct on the Internet.

The march of technology demands the enactment of newer legislation both to regulate the technology and also to facilitate its growth. The next to be soon seen in the statute book is the Act on Communication Convergence, which since 2001 is a Bill. This Act proposes to facilitate development of a national infrastructure for an information based society, and to enable access thereto; to provide a choice of services to the people with a view to promoting plurality of news, views and information; to establish a regulatory framework for carriage and content of communications in the scenario of convergence of telecommunications, broadcasting, data-communication, multimedia and other related technologies and services; and to provide for the powers, procedures and functions of a single regulatory and licensing authority and of the Appellate Tribunal. The communications commission is the key institution in the Bill that is responsible for all matters relating to regulation of communications. Among its main functions are to ensure:

- i) that the communication sector is developed in a competitive environment and in consumer interest;
- ii) that communication services are made available at affordable cost to all, especially uncovered areas including the rural, remote, hilly and tribal areas;
- iii) that there is increasing access to information for greater empowerment of citizens and towards economic development;
- iv) that quality, plurality, diversity and choice of services are promoted;
- v) that a modern and effective communication infrastructure is established taking into account the convergence of information technology, media, telecommunication and consumer electronics;
- vi) that defense and security interests of the country are fully protected;
- vii) that introduction of new technologies, investment in services and infrastructure and maximization of communication facilities and services (including telephone density) are encouraged;
- viii) that equitable, non-discriminatory interconnection across various networks is promoted;
- ix) that licensing and registration criteria are transparent and made known to the public;
- x) that an open licensing policy allowing any number of new entrants is in place; and
- xi) that the principle of a level playing field for all operators, including existing operators on the date of commencement of this Act, is promoted, so as to serve consumer interest.

Please answer the following Self Assessment Question.

**Domestic Laws:
Backgrounder**

<p>Self Assessment Question 1 <i>Spend 3 Min.</i></p> <p>Discuss the reason which necessitate the regulation of cyberspace.</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>

1.4 INFORMATION TECHNOLOGY ACT, 2000

The Ministry of Information Technology was formed in 1999 burdened with the enormous duty of making India an IT super power by 2008. In less than a year, India witnessed the enactment of its first statute relating to information technology¹ on the pattern of the Model Law on Electronic Commerce, 1996, adopted by the United Nations Commission on International Trade Law. The Electronic Transactions Act, 1998 of Singapore also significantly guided the framing of the Act. The Information Technology Act, 2000 was passed by Parliament on May 15, 2000, approved by the President on June 9, 2000 and notified to come into force on October 17, 2000.

The Information Technology Act intends to give legal recognition to e-commerce and e-governance and facilitate its development as an alternate to paper based traditional methods. The Act has adopted a functional equivalents approach in which paper based requirements such as documents, records and signatures are replaced with their electronic counterparts. The Act seeks to protect this advancement in technology by defining crimes, prescribing punishments, laying down procedures for investigation and forming regulatory authorities. 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 too have been suitably amended in order to facilitate collection of evidence in fighting electronic crimes.

1.4.1 A Quick Overview of the Act

Section 1 deals with the extent, commencement and application of the Act. It also specifically prohibits the application in certain situations. Section 2 of the Act deals with definitions. Digital Signature has been vastly covered under Chapters II, VI, VII and VIII. Chapters III and IV exclusively deal with electronic records. Chapter V introduces the concept of secure electronic records and secure digital signatures as also the security procedure. Offences and Penalties under the Act have been enumerated in Chapters IX and XI whereas the Cyber Regulations Appellate Tribunal, its constitution, powers and functions have been laid down in Chapter X. Chapter XII deals with the issue of liability of network service providers. Finally, 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 indicated above. This is the span of the Act. In the following discussion, though relevant definitions would be given either in the running paragraphs, or in the footnotes, still, for quick reference, the reader is advised to refer to section 2 of the IT Act and the Glossary given in Schedule V of the Information Technology (Certifying Authorities) Rules. A detailed discussion of the Act is attempted in the next two units.

Please answer the following Self Assessment Question.

Self Assessment Question 2*Spend 3 Min.*

Discuss the salient features of the Information Technology Act, 2000.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

1.5 CRITIQUES OF THE I.T. ACT

The IT Act, 2000 came at a time when cyber-specific legislation was much needed. Moreover India was one of the earliest countries to draft a legislation of this kind. Without a doubt, the IT Act has not only helped India achieve the position that it holds today in the IT sector but also helped overseas based IT

and related investors gather a favourable impression of India's IT related legal system, and therefore make a decision to invest in India. While a lot can be said the merits of the Act, there is room for some improvement too.

One of the main drawbacks of the Act seems to be its inadequacy in providing sufficient data protection provisions. With the transformation of the Internet into the main arena of conduct of economic activities, there is a danger of the possibility of key data being the target of crooks, for snooping paparazzi, for espionage agencies etc.

The IT Act does not offer much in terms of protection of intellectual property on the net. In other words there are no provisions in the act to protect copyrights, patents or trademarks. To take a more specific example, the Act has no provisions to deal with what is known as 'cyber squatting' relating to domain name disputes. Though the area is presently covered laws relating to intellectual property like Trade Marks, it is desirable for the IT Act also to have such a provision. For instance when a major company wishes to register a domain name in lets say .in, and it suddenly finds someone else wholly unconnected to the company having registered the name of the company in that category, the company has no remedy under the IT Act though it has the trademark for that name. Similarly, there are no provisions in the IT Act to address cyber theft, cyber stalking, cyber defamation etc.

On privacy issues also the Act has come in for a lot of flak. It does not prohibit behaviour like spams and unsolicited e-mails that flood one's in-box. Neither does it provide for instances where there is a misuse of confidential private data collected online.

The IT Act also is silent on issues relating to cross border taxation arising out of international trade, which in the long run is inevitable and would turn out to be a contentious issue.

Even from the purely technological standpoint there is a criticism that the Act binds digital signatures to the asymmetric encryption system, limiting the scope of innovation in technology. This is a drawback given the fact that technology is constantly changing with one system giving place to another.

A single section devoted to liability of the Network Service Provider is highly inadequate. The issues are many more. Apart from classification of the Network Service Providers itself, there are various instances in which the Provider can be made liable especially under other enactments like the Copyright Act or the Trademark Act. However, the provision in the IT Act, 2000 devoted to ISP protection against any liability is restricted only to the Act or rules or regulations made thereunder. The section (though it might be argued the other way round, still) is not very clear as to whether the protection for the ISPs extends even under the other enactments.

There has been a general criticism of the wide powers given to the police under the Act. Fear, especially among cyber café owners, regarding misuse of powers under the IT Act, 2000 is not misplaced. Anyone can be searched and arrested without any warrant at any point of time in a public place. But at the

same time, the fact that committing a computer crime over the net and the possibility of escaping thereafter is so much more viable, that providing such policing powers to check the menace of computer crimes is also equally important. Again, interception of electronic messages and e-mails might be necessary under certain situations but the authorities cannot be given a free-hand in interception as and when they feel. Similarly, we need to enquire and delve deeper into police powers of investigation, search and warrant under the IT Act, 2000 and look for a more balanced solution.

Another criticism of the Act seems to be that offences can be prosecuted both under the civil and the criminal procedure system. Some of the instances that provide for fine would have to be taken as per provisions of the civil procedure code which is generally perceived to be a slow process. Other offences that involve punishments of imprisonment would be as per the provisions of the Criminal Procedure Code.

Finally, how the Act will be interpreted by a court of law and its implementation and flaws in the long run are yet to be tested on a case-specific factual terrain as the number of cases that have come before the higher courts under the Act is just a handful.

1.6 PROPOSED AMENDMENTS TO THE I.T. ACT

With an objective to review the Information Technology Act 2000, in the light of the latest developments and to consider the feedback received for removal of certain deficiencies, an expert committee under the Chairmanship of Shri. Brijesh Kumar, Secretary, Department of Information Technology was set up. The committee had during its deliberations analysed some of the relevant experiences and international best practices. The Committees recommendations have been with the twin objectives of using the IT as a tool for socio-economic development and employment generation, and also to further consolidate India's position as a major global player in the IT sector.

As the technologies and applications in IT sector change very rapidly, some of the provisions related parameters that may change from time to time have been proposed to be amended to provide for the new developments to be incorporated by changes in rules/govt notifications. This would enable law to be amended and approved much faster and would keep our laws in line with the changing technological environment. The Act is proposed to be made technology neutral with minimum change in the existing IT Act 2000. One major change proposed is the substitution of "digital signature" with "electronic signature" through an amendment to section 4. Digital signature is thus recognised as one of the types of electronic authentication of records and not as the only way. This is more in the nature of an enabling provision so as to include more forms of authentication as and when technology advances. Further in order to allow public-private partnership in e-governance delivery of services, certain amendments have been proposed.

A new chapter (III A) under the title "Electronic Contracts" is proposed to be added with section 10 proposing to give validity to Electronic Contracts. Another impetus to e-commerce is sought to be given through this amendment.

- 1) Laws may be technology neutral such as laws relating to defamation, forgery, contract company etc. Here it is immaterial whether activities covered by these acts are performed on the Internet or not.
 - 2) Laws relating to the activities which can be performed on the Internet only such as hacking, denial of services, viruses etc.
- Cyber laws in the domestic field consist of the IT Act supplemented by a wide number of other Acts.
 - The Act gives legal recognition to e-commerce, e-governance, digital signature keeping records in electronic form etc. It also defines crimes relating to computer and Internet and makes provisions for their investigation and makes provision for punishment.
 - We have also seen that the IT Act has a lot of scope for improvement and that an amendment is already in the cards. The expert committee set up by the government has suggested making the Act more technology neutral. Some of the amendments suggested by the committee are — replacement of the word — digital signature by electronic signature, making provision for electronic contract, child pornography, etc.

1.8 TERMINAL QUESTIONS

- 1) Discuss the need of special laws in the field of cyberspace? Do you think that Indian laws sufficiently deal with every aspect of the challenges posed by the technology in the field of cyberspace?

1.9 ANSWERS AND HINTS

1. Phenomenal growth in the use of Internet in almost every walk of life has posed the challenge of regulating the cyberspace. Such as identity of the person, electronic signature in the contract and other transactions on the Internet, hacking, virus etc. therefore special legal provisions are needed to cope with it.
Indian IT Act has tried to address these issues but more needs to be done. Government set up a committee to suggest amendment in the act. Committee made valuable suggestions which should be incorporated in any future amendment to the Act.
- 2) Section 1 deals with the extent, commencement and application of the Act. It also specifically prohibits the application in certain situations. Section 2 of the Act deals with definitions. Digital Signature has been vastly covered under Chapters II, VI, VII and VIII. Chapters III and IV exclusively deal with electronic records. Chapter V introduces the concept of secure electronic records and secure digital signatures as also the security procedure. Offences and Penalties under the Act have been enumerated in Chapters IX and XI whereas the Cyber Regulations Appellate Tribunal, its constitution, powers and functions have been laid down in Chapter X. Chapter XII deals with the issue of liability of network service providers. Finally, 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 indicated above. This is the span of the Act. In the following discussion, though relevant definitions would be given either in the running paragraphs, or in the footnotes, still, for quick reference, the reader is advised to refer to section 2 of the IT Act and the Glossary given in Schedule V of the Information Technology (Certifying Authorities) Rules. A detailed discussion of the Act is in the next two units.

- 3) With an objective to review the Information Technology Act 2000, in the light of the latest developments and to consider the feedback received for removal of certain deficiencies, an expert committee under the Chairmanship of Shri. Brijesh Kumar, Secretary Department of Information Technology was set up. The committee had during its deliberations analysed some of the relevant experiences and international best practices. The Committees recommendations have been with the twin objective of: using the IT as a tool for socio-economic development and employment generation, and also to further consolidate India's position as a major global player in the IT sector.

A new chapter (III A) under the title "Electronic Contracts" is proposed to be added with section 10 proposing to give validity to Electronic Contracts. Another impetus to e-commerce is sought to be given through this amendment.

In view of the concerns about the operating provisions in the IT act related to data protection and privacy, in addition to contractual agreements between parties, the existing Sections for instance 43, 65, 66 and 72 have been revisited and some amendments have been proposed. A new section is being added (Sec 67(2)) to address child pornography with higher punishment and fine of global standards. So also now a new form of illegal conduct called video voyeurism, which is capturing the private area of an individual without his consent and then transmitting it, has been included as a punishable conduct.

1.10 REFERENCES AND SUGGESTED READINGS

Under the Act, the 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, 2001; and, (d) the Guidelines for Submission of Application for Certifying Authority, 2001.

**Domestic Laws:
Backgrounder**