UNIT 9 INTRODUCTION TO DATA

Structure

9.1 INTRODUCTION

The transmission and storage of data has undergone a radical change due to advances in technology and technological processes. The information technology revolution has made the personal computer as common as a fountain pen and the individual more and more dependent on a number of public and private services for example, banking, credit, social security, insurance, employment, direct marketing, statistics, police, telecommunications etc. that operate with automated administrations. Owing to the relatively much faster transmissibility and easier storage of data in today's scenario, it has become imperative to both prevent and shield data from unauthorized access and usage. The increased usage of the automated form of processing personal data over the past few decades has in particular enhanced the risk of illegal use of personal data by facilitating its transfer between countries with great differences in the level of protection provided to personal data.

The concept of data protection has thus gained critical importance to ensure that personal data is not processed in a manner that is likely to infringe or invade personal integrity and privacy. The concept of protecting data, though in its early stages of practice, promises on one hand, rapid growth over the coming years to secure for every individual, whatever the nationality or residence, respect for such individual's rights and fundamental freedoms, and in particular the right to privacy, with regard to the automatic processing of personal data relating to such individual. However, on the other hand, to be able to

ensure that the right to privacy, and the protection of personal data in particular, are respected in the electronic superhighways capable of transferring a vast amount of personal information worldwide in real time at very high speed shall be a pertinent challenge. Data protection has thus become a topical subject, with an ever-increasing number of evolving practical questions getting attached to it.[1]

Before, we study the concept and the measures taken to regulate data protection in detail, let us first understand what is meant by "data".

9.2 OBJECTIVES

After studying this unit, you should be able to :

- explain the meaning of the term 'data';
- explain the concept of data protection;
- comprehend the need to regulate data protection;
- enlist the measures taken by UK, US and India to regulate data protection; and
- explain the current status of data protection regulation in India.

9.3 MEANING OF 'DATA'

The Oxford English Dictionary defines the term "data" to connote things given or granted; things known or assumed as facts and made the basis of reasoning or calculation; facts collected together for reference or information; quantities, characters or symbols on which operations are performed by computers and other automatic equipment, and which may be stored and transmitted in the form of electrical signals, records on magnetic, optical or mechanical recording media, etc.

Further, the term "data" has been defined in a number of legislations worldwide, which signifies its importance in today's day and age. It may be relevant to look at some of these definitions.

Section 2 (1) (o) of the (Indian) Information Technology Act, 2000 (Act) defines "data" to mean a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

The United Kingdom Data Protection Act, 1998 (UK Act) defines data as information which-

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record.

The UK Act further defines "personal data" as data, which relates to a living individual who can be identified

(a) from the data, or

(b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

(c) and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

In view of the information revolution, which has resulted from the coupling of computer techniques, telecommunications, multimedia and the lightning development of the Internet, the legislations have also therefore laid stress and emphasis on the computer- processed and computer stored forms of data.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Can data under the UK Act be information that does not form part of an accessible record?

.....

.....

.....

.....

.....

.....

9.4 NEED FOR REGULATION OF DATA PROTECTION

It is well understood that the free flow of information has contributed to the globalisation and virtualisation of society and thus has raised concerns about security, respect of fundamental rights and privacy. The keeping of records on individuals for various purposes and the risks of infringement of privacy, by both public and private sectors, have never been easier than today, through the use of new technologies and the convergence of their application. One example of such infringement of privacy is often reflected in a number of unidentified calls received by consumers today from a number of companies selling their products on telephone and through e-mails on the basis of the data collected by them through sources which are not disclosed to consumers. Therefore, an active policy and awareness by and on behalf of citizens is constantly a necessity.

A core problem in this respect concerns what forms of regulation actually benefits citizens and how their interests can be determined. Further, as data protection is in the interest of the citizen this regulation must, as a starting point be acceptable. However, there are several conflicting interests that are active within this field and it is a constant battle to ensure that these interests are balanced and that those of citizens are sufficiently protected. In view of this, it is further important to look at the efforts made for regulation and protection of data internationally.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 2 Min.*

Provide an example for a common infringement of privacy today?

.....

.....

.....

.....

.....

.....

9.5 REGULATION OF DATA PROTECTION

9.5.1 European Union

In the European Union (EU), the protection of personal information became widespread after the Second World War. The explosion of information power brought about by computing established fears that the usage of the new machines might weaken or undermine individual human rights which surfaced quite early in mainland Europe. Europe had only established its Human Rights Commission in the 1950s after the European Convention for the Protection of Rights and Fundamental Freedoms was adopted in 1950. The suggestion that data movements might be curtailed or controlled on human rights grounds gave rise, in its turn, to reservations of a different kind; such as trade being fettered if information could not flow freely. The development of standards for the use and dissemination of personal data, or data protection standards, proved to be the response to these apprehensions. The standards laid by the European Union are seen embodied in enforceable laws throughout Europe and in many other parts of the world.

9.5.2 OECD Guidelines

It was in the year 1980 that an international team of experts convened by the Organization of Economic Co-operation and Development (OECD), developed a set of privacy guidelines, consisting of a total of eight "privacy principles" and enforcement approaches. The OECD Guidelines were intended to offer harmonised protection of individual privacy rights while simultaneously being flexible enough to apply across a variety of social, legal, and economic circumstances. The 1980 OECD Guidelines have had an enormous influence in finding their way into a variety of legislative and self-regulatory adaptations. The following are the eight broad principles pertaining to privacy laid down by OECD:

1. *Collection limitation*: There should be limits on data collection, and data should be obtained by fair and lawful means and, where appropriate, with the knowledge or consent of the data subject.
2. *Data quality*: Data should be relevant to the purpose for which it is collected and should be accurate, complete, and up to date.
3. *Purpose specification and notice*: The purpose for which data are collected should be provided to the data subject not later than at the time of collection; the subsequent use of data should be limited to those and other "not incompatible" purposes.

4. *Use limitation*: Data should not be disclosed or used except for purposes specified in the notice unless the data subject consents or the law requires disclosure.
5. *Security*: Requires "reasonable" safeguards for personal data.
6. *Openness*: Requires openness about practices and policies regarding personal data; it should be made easy to identify a data controller, how to reach it, the kinds of data it collects and the main purposes of that collection.
7. *Access*: Requires "reasonable" access by a person to data collected, or information about that data, and right to challenge, including requiring erasure of inaccurate data.
8. *Accountability*: The data "controller" should be accountable for complying with the protections and should be liable for harm.

The data protection principles and legislations in general have thus been founded upon the Guidelines on the Protection of Privacy and Trans border Flows of Personal Data issued in 1980 by the OECD. The OECD Guidelines will be studied in greater detail in the next unit.

9.5.3 EU Directive

In 1995, the EU adopted its data protection directive (95/46/EC), and established a detailed privacy regulatory structure for prospective and intended adoption into national law by EU member states. The directive adopted the OECD concepts on data protection in its directive. However, the directive made several important changes or additions to the OECD Guidelines such as the creation of a "legitimacy" principle which prohibits any data to be processed that does not have a legitimate purpose. It further interpreted the openness principle to require national registration of databases and data controllers and promoted the free flow of information only between and amongst the EU member states. The cross border transfer to other countries was prohibited unless the other country provided an "adequate" level of protection, although the same was made subject to certain exceptions. Lastly the directive specifically stated that the member states should encourage the use of codes of conduct thereby providing a means to limit the possible discretionary exercise of authority and also obtaining flexible means to update national interpretations.

The EU member states have a tradition of industry- government dialogue and the use of industry codes of conduct. The EU directive explicitly encourages the use of such "self-regulatory" measures; thereby making the impact of the directive less burdensome. In other words, these codes allow regulatory measures to be flexible in order to keep pace with technological developments and with evolving industry practices. These codes further assist in avoiding unnecessary regulatory barriers and limiting the discretionary exercise of regulatory authority.

This directive was thus an important initiative to protect personal information by prohibiting the transfer of such personal data to those countries, which did not conform to the privacy protection requirements of the EU[2].

9.5.4 United Kingdom

UK enacted the UK Data Protection Act, 1984 as amended by the UK Data Protection Act, 1998 (DPA). The 1984 Act drew on both the OECD and Council of Europe principles. It sets out eight principles for data handling, largely drawn from the two international instruments and state that the personal data should be:

(a) lawfully processed;

(b) lawfully obtained;

(c) adequate and relevant;

(d) accurate and upto date;

(e) stored for a specific purpose and a reasonable duration;

(f) processed in accordance with the rights of the owners of such data;

(g) appropriate technical and organizational measures should protect against unauthorized use of such data and provide overall protection; and

(h) transborder flow of information between countries with similar levels of protection.

The DPA provides a fairly detailed route map wherein various measures of protecting personal information / individual privacy are set out. These eight principles provide legal, technical and contractual protection to personal data and further also state the parameters within which personal data is to be processed, obtained, stored and used in the public domain. These principles also govern data exchange beyond the national level to protect information crossing the local borders. Indeed a comprehensive protection is put forth within these principles for personal data. Any contravention of the rights of the individual owning personal data is subject to compensation for the extent of damage.

9.5.5 United States

In the United States however, privacy protection is implanted in a much longer historical development path as the same was developed in a fragmented manner commencing from the basic principles of tort law and as a by- product of industry-specific legislation, such as the Fair Credit Reporting Act.

The US currently has no legislation specific to consumer data privacy protection, relying instead upon the industry self-regulation approach to the OECD Guidelines. Having stated that however, due to immense pressure to strengthen consumer data protection owing to the looming threat of the requirements of the EU data directive, the Federal Trade Commission (FTC) has taken a more proactive approach in protecting consumer data, acting pursuant to its authority to prevent unfair and deceptive trade practices in accordance with the FTC Act[3].

9.5.6 Asia Pacific

In November 2004, the Asia-Pacific Economic Cooperation (APEC), a forum established in 1989 for facilitating economic growth, co-operation, trade and investment in the Asia Pacific Region endorsed a privacy framework which is based on the principle structure and import upon the core fundamentals of the OECD Guidelines. The same recognises "reasonable expectation" of privacy and gives due emphasis to the benefits of participation in a global information economy. It specifically endorses "proportionality" in terms of national regulation so that regulation and remedy are proportional to the likelihood and significance of causing harm to an individual subject. The framework further focuses upon the "core fundamentals" of the OECD Guidelines and on the use of the internet to provide notice, consent, and control.

It may be noted that like the OECD, the APEC is only a inter governmental grouping and operates on the basis of non-binding commitments, open dialogue and equal respect for the views of all participants[4].

9.5.7 India

Currently there are no specific "data protection" specific laws in India. However, in the absence of specific laws, the Indian judicial system offers a few stand-in laws and other indirect safeguards e.g. Information Technology Act, 2000 and the Indian Penal Code, 1860, all of which are discussed in detail in the succeeding units.

However, recognising the need for data protection in the technological environment, the Central Government has taken several initiatives for the furtherance of data protection. Some of the initiatives taken by the Ministry of Information Technology in India may be mentioned:

- *Standardisation, Testing and Quality Certification (STQC) Directorate*

Due to the international demand that Indian firms should have an international security standard accreditation, the Indian government has set up the Standardisation, Testing and Quality Certification (STQC) Directorate (under the Department of Information Technology (DIT)). The Directorate has been able to launch an independent third-party certification scheme for the Information Security Management System, as per BS 7799 Part 2, and has achieved international recognition in the form of accreditation from the RvA, Netherlands.

- *Computer Emergency Response Team (CERT)*

The Indian Computer Emergency Response Team (CERT) was established by the DIT to be a part of the international CERT community. CERT was set up to protect India's IT assets against viruses and other security threats.

- *Information Security Technology Development Council (ISTDC)*

The Ministry has recently set up the Information Security Technology Development Council (ISTDC). The main objective of this program is to facilitate, coordinate and promote technological advancements, and to respond to information security incidents, threats and attacks at the national level (Check Regulations in India - http://www.nasscom.org).

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What are the principles for data handing set out in the DPA?

.....

.....

.....

.....

.....

.....

9.6 MONITORING OF DATA PROTECTION

The whole issue of data protection in the digital context probably hinges on the contention of the interests of the individual versus the state, market and technology developments.

Organizations require to look now at how they collect, store and use personal data and comply with existing laws and in absence of such laws, ask themselves whether they are adhering to the ethical norms or not. It is therefore obligatory, both legally and morally, for the persons possessing and handling data to monitor data protection processes holistically and in real time. It is expected that this will help in achieving improved reliability and faster problem resolution.

Data protection monitoring and tuning work will not only include the help of advanced system information processing and monitoring devises and software but also the human factor, which is more critical. It cannot be denied that the sheer amount of data is growing rapidly, and storage, replicating and transmitting technologies are advancing quickly. This makes it imperative to design the storage infrastructure for the future, as well as for meeting present needs. The infrastructure also needs to scale and adapt, as data protection needs change.

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 3 Min.*

State the two critical factors that seek to assist in monitoring of data protection?

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

9.7 SUMMARY

- Faster transmissibility and easier storage of data has increased the requirement to prevent and shield data from unauthorized access and usage.
- Data protection while securing respect for and individual's rights raises the question as to whether the protection it seeks to offer shall merit respect and acknowledgement in the practical scenario of information transmissibility.
- Data is a representation of information and knowledge intended to be processed by means of equipment and is recorded in varying forms.
- Regulation of data protection is necessary on account of the free flow of information that has raised concerns about security, privacy and respect of fundamental rights.
- The European Union initiated data protection laying standards embodied in various legislation subsequent thereto across the world.
- OECD has set down 8 principles pertaining to privacy
  - Collection limitation
  - Data Quality
  - Purpose specification and notice

- Use limitation
- Security
- Openness
- Access
- Accountability

- The EU Data Protection directive adopted the OCED concepts however, made alterations such as creation of "legitimacy" principles and requiring transferee countries to provide adequate protection in case of cross border transfer of data.
- The UK has set out 8 principles for data handling
  (i) lawfully processed
  (ii) lawfully obtained
  (iii) adequate and relevant
  (iv) accurate and up to date
  (v) stored for specific purpose and reasonable duration
  (vi) processed in accordance with owners rights
  (vii) stress on technical and organizational measures
  (viii) transborder flow between countries
- The US relies on industry self regulatory approach to the OCED Guidelines having no specific legislation of its own. The FTC imposes a proactive approach.
- APEC endorses a privacy framework based on the core fundamentals of the OECD Guidelines.
- India has no data protection laws however, the central government has taken several initiatives such as setting up the STQC Directorate, the CERT and the ISTDC.
- Data protection monitoring requires both advanced system information processing and human intervention.

9.8 TERMINAL QUESTIONS

1. Explain the term 'data' with reference to various Acts?
2. What is the requirement for regulation of Data Protection? Explain briefly keeping in mind the EU Directive and the UK Data Protection Act.
3. How have the OECD guidelines helped in harmonising protection of individual privacy?
4. What is the current status of 'data protection' laws in India?
5. Summarize the concept of 'data protection'?

9.9 ANSWERS AND HINTS

Self Assessment Questions

1. No 'Data' under the provisions of the UK Act, cannot be an information that does not form part of an accessible record.
2. An example of common infringement of privacy is reflected in a number of unidentified calls received from consumers today by number of companies selling

their products on telephone and through e-mails on the basis of the data collected by them through sources which are not disclosed to consumers.

3. The eight principles set out under the DPA for data handling are:
   (a) Lawfully processed
   (b) Lawfully obtained
   (c) Adequate and relevant
   (d) Accurate and up to date
   (e) Stored for specific purpose and reasonable duration
   (f) Processed in accordance with the rights of owners of such data
   (g) Appropriate technical and organizational measures should protect against unauthorized use of such data and provide overall protection
   (h) Transborder flow of information between countries with similar levels of protection.
4. The two critical factors are advanced system information processing and monitoring devices and software and the human factor.

Terminal Questions

1. Refer to section 9.3 of the unit.
2. Refer to section 9.4 of the unit.
3. Refer to section 9.5 of the unit.
4. Refer to section 9.5 of the unit.

9.10 REFERENCES AND SUGGESTED READINGS

1. Blume, P. "The Citizen's Data Protection". The Journal of Information, Law and Technology (JILT). 1 (1998). 10 Mar. 2007 <http://www2.warwick.ac.uk/fa soc/ law/elj /jilt/1998_1/ blume/>.

2. Legal Site Check. 10 Mar. 2007<http://www.legalsitecheck.com dataprotection.html>.

3. Ibid.

4. Supra n.2.