Data Protection and Privacy in Cyberspace- National and International perspective

Dr. Deepti Khubalkar
Assistant Professor in Law, Symbiosis Law School, Symbiosis International (Deemed University), Mouza-Bhandewadi, Wathoda, Nagpur-440008, Maharashtra State, India
deeptikhubalkar@gmail.com

ABSTRACT

Data protection and data privacy issues including the compliance is becoming utmost important especially during Covid-19 pandemic where all are majorly relying on internet and online platforms. This chapter highlight the importance of legal framework in India to provide protection for consumers and privacy considerations for organisations with respect to electronic data. This chapter also talks about the lack of mechanism to compel organisations carrying data to delete or remove if there is no compelling reason for an organization to carry on processing it including the sensitive, personal data and privacy policies and liabilities. This chapter also analyse the present legal protection to data privacy in India and bill relating to data protection and privacy in India which is almost ready to be implemented. In this chapter author also attempting to explore the European union laws of data protection.
The objective of this chapter is to understand and explore the right to privacy and its application on data protection in cyberspace and how they link up, how it evolved during the time, essence of the Personal Data Protection bill and liability and role of internet service providers. This Chapter will also attempt to highlight the importance of data protection and intellectual property rights and related patent law and procedural issues.

Keywords
Data privacy, organisation, Information Technology, Data protection, consumers, e-commerce, cybespace

Article Received: 10 August 2020, Revised: 25 October 2020, Accepted: 18 November 2020

Introduction

Data protection law gives people rights in their personal information, and it restricts the ways in which business organizations can use people's personal information. With the advent of internet technology e-commerce has developed drastically in recent years giving tremendous opportunity to business owner to reach customer globally. Abuse of data and deceptive marketing for the growth of business are the biggest threat to e-commerce. Trust building in international customer is not an easy task even in the era of globalization without providing proper mechanism to protect the data and privacy to customer data. European Union has recently passed a legislation for this purpose and to replace the old data protection law with General Data Protection Regulation(GDPR).

Theoretical Background

For the purpose of economic security. General Assembly of United Nations, resolves for unification of international trade. With this objective, UNCITRAL is created under which various conventions relating to international business were conducted.
In 1984, Secretary-General submitted a report titled "legal aspect of automatic data processing". This report indicated various important issues relating to computer records and its legal sanctity, some business transactions and contract requires legal necessity of writing, registration, signature, general elements of validity and liability. The Secretariat of the commission prepared a report on "legal value of computer records" and submitted it to the commission for its consideration. Report observed that less use of computer and technology is because of lack of legal protection in the field. After the perusal of the report prepared by the Secretariat on the validity of computer records, commission considered the following issues;

- That, the use of automatic data processing (ADP) is in near future likely to be widely used in international trade and administrative services.
- That, the legal requirement of paper documentation is a hurdle in efficient use of ADP as it create insecurity for its application.
- That, existing rules of evidence apply only document based evidence and not computer based record.
- That, there is a need to adopt and increase the reliability in the use of ADP for encouraging its application.

On the basis of above considerations need of some changes in existing laws was felt and accordingly recommendations were made by the commission for bringing changes in rule of evidence to include computer record as admissible evidence in court of law. For that purpose, states were urged to implement these changes in the laws so that parties will be enabled to transmit data with more security. It is further recommended that the authentication of electronic signatures should be facilitated. It is specifically commanded that existing legal text be modified to review the existing legal provisions which require that government documents should be in writing and manually signed. The recommendations were also made to international organisation related to the legal field.
Therefore, the above recommendations were adopted by the Gen Assembly by passing a resolution urging government and international organisation to take action. However, these could not bring any improvement in domestic laws and the legal requirement of paper-based document and the

signature and hence it remained the same. It is found that recommendations of 1985 were of without any suggested measures for its implementation. Hence, commission in 1988 decided to consider the above issue with a fresh look. The Secretariat of the commission was unsigned the job to prepare a preliminary report on the issue of formation of contracts through electronic medium, developing technology and traditional paper-based laws, and urgency of legal rules.
The Secretariat found that there are a number of standard interchange agreements and therefore, it is greatly responsible for not establishing a legal framework to suit the business of electronic commerce. The Secretariat in its report suggested that there is a need to provide a legal framework for the electronic commerce and for that purpose the commission should prepare a standard communication agreement by involving all legal systems particularly developing nations who are likely to face the similar problem very soon in near future with respect to electronic transactions.
On these recommendations, job of preparation of legal rules on electronic data interchange was unsigned to working group on electronic data interchange. The group completed the work and prepared legal rules for "electronic data interchange" (EDI) and other modern means of communication. The main purpose of this was to create a legal framework to deal with electronic commerce. After approval of this Model Law it was sent for the comment of all governments and international organisations.
The General Assembly passed a resolution to give effect to the model law on electronic commerce so that all the States dealing with electronic commerce with divergent laws can achieve uniformity in legal framework with respect to electronic commerce and related issues. Therefore, it is recommended to states that whenever they enact law on the present issue of positive consideration be given to the model law to maintain uniformity of laws relating to electronic commerce including storage of information at the global level.
Thus to execute the UNCITRAL Model Law on electronic commerce, Information Technology Act 2000 is passed. Certain corrections were made in the year 2008 by way of amendment. Originally the act was passed to recognise electronic commerce.

Data protection under Information Technology Act 2000

Under I T Act, 2000, few provisions are specifically provided for the purpose of data privacy in specific sense. Section 72 of the IT Act imposes liability for breach of confidentiality and privacy.
Section 43A also imposes liability for breach of protection of data but limited upto the nature of sensitive personal information only. Any corporate body handling such data is responsible to protect its privacy.
This sensitive data protection rule of 2011 defines sensitive personal data or information under section 3 includes personal information including financial and private information of people .
Recently, a Bill to protect Data is introduced in the house named The Personal Data (Protection) Bill, 2019. The Bill does not provide any definition of privacy however; it focuses on the protection of personal and sensitive personal data of person. Bill proposes to give overriding effect on all existing provisions directly or remotely related to privacy. It proposes to prohibit that no person shall collect share, process disclose or otherwise handle any personal data of another person except in accordance with the provision of proposed Bill. The Bill proposes security to the personal data of citizens. It is pertinent to note that no privacy protection is provided to data on social media. Even the government under the scheme of Aadhar Card, collecting information of citizens without ensuring protection of security. The Bill defines the term 'Personal Data' to include Biometric data, sexual preferences, medical history and health, political affiliation, religion, race, caste, financial and credit information. This definition differs from the definition provided in the Reasonable Security Protection and Procedure and Sensitive Personal Data and Information Rule 2011. Thus the ambit of personal data has been enhanced in the Bill.
Bill also proposes certain exceptions to the violation of privacy of data on the grounds of medical emergency, national security, to prosecute for cognizable offence etc. The Bill provides that when offence is committed person will be strictlycriminally liable for imprisonment and fine. It requires no assessment of intention or mens rea.

Significance of European Union in data protection: GDPR

The former EU data protection law that abolished by GDPR (General Data Protection Regulation) and upon which the UK's Data Protection Act 1998 was based remain substantially the same under the new law. This mainly includes, the obligation to ensure that only a minimum quantity of data are used for any particular purpose, the obligation to process only such information on people as is relevant to the purpose of the processing, the obligation to supply a copy of their personal data to anyone making a request (data subject access), the obligation to apply appropriate security provisions to personal data processing, and the obligation to destroy or delete data held after they have become obsolete.
Some of the new obligations, such as the requirement to conduct data protection impact assessments are only new in terms of the obligation to carry them out. They are new in terms of their concept. For example, many organizations had been conducting DPIAs previously known as privacy impact assessments for many years prior to the GDPR's inception.
The main principle of this is the protection of an individual's privacy in relation to the processing of personal data; and the harmonization of data protection laws of the member states. These laws are primarily applied to organisations located in the European Union, hence organisations will have to comply with data protection legal requirements. GDPR has wider applicability but does not include controller situated outside EU organisation.

Jurisdiction Challenges in data protection

Since cyber world has no boundaries, it is a herculean task to frame laws to cover each and every aspect. Moreover,

with the increased use of Internet, direct satellite connections between countries, increasingly shrinking the gap of communication between countries, and is becoming a global village. However, determination of jurisdiction of particular transaction is of utmost necessary. The traditional rule of jurisdiction in civil and criminal cases, gives no effective remedy to the parties of Internet dispute. I.T. Act 2000 has no specific direction with respect to application of the rules of jurisdiction, especially in the context of violation of trans boundary laws of domestic legislation.

Traditional rule of jurisdiction in Indian legal system are governed in two ways; civil law jurisdiction and criminal law jurisdiction. In civil cases it depends upon the agreement between the parties and in its absence as per the provision of the law which basically depends upon subject matter (movable / immovable property) , pecuniary value of the case, residential status of the parties, authority of the court on the basis of territorial limit and finally on the basis of cause of action. In criminal cases, it depends upon the place where the offence has been committed. Thus, applicability of law depends upon geographical limitations. Thus, civil jurisdiction is divided into various categories.

Jurisdiction is always subject to territory of the state. There is a hierarchy of courts i.e. Civil Court / Magistrate-senior Civil Judge/Session Court-High Court –Supreme Court. All these courts act as per the territorial jurisdiction except Supreme Court. Pecuniary jurisdiction is a power of court to decide a civil case based on amount claim in the suit. It prescribes limitation to grant relief up to the prescribed amount. Subject matter jurisdiction means the place of subject matter, which determines the power of the court. In case of no subject matter, jurisdiction of court is determined on the basis of cause of action.

The nature of the Internet allows transnational interaction of persons. Each country has its own set of rules applicable on person within its own geographical limits. Consequences of the circumstances lead to applicability of different sets of laws for implementation of provision of it. Person interacting with other in transnational transaction believes that law of his country will apply to their action. But nature of interaction through Internet sometimes violates the law of other country unknowingly.

Current legal setup does not allow the courts to try offences committed beyond the territorial limits of the court. Section 75 of Information Technology Act 2000 provides that the

“Act shall apply to an offence or contravention which involves a computer, computer system or computer network located in India, committed outside India by any person irrespective of his nationality if the act or conduct constitutes the offence or contravention”.

This provision prima-facie shows that court can assume jurisdiction over a transnational cyber offence on the strength of the provision of Information Technology Act 2000. Information Technology Act 2000, however, does not mention the rule of application with regard to jurisdiction over the Internet. There have been few cases in the Indian courts where the need for the Indian courts to assume jurisdiction over foreign subject has arisen.

Conclusion

India does not have specific privacy legislation other than few provisions in IT Act and other piecemeal provisions of data protection. However, in absence of strong data protection law, abuse of this information can be foreseen.

IT Act in India, has few provisions of data protection but has a limit to cover all the protection measures required for data security especially in transnational electronic commerce. A wide range of instances are an example to show that there are violation of data protection laws and processing of data with advent of new technology. Further the penalty imposed under IT law for violation of privacy to data by e-commerce is unable to give adequate deterrence. With the increase use of internet and people’s reliance on e-commerce sites needs adequate data security regime which should provide strong rights in favour of individuals so that they can get redress against security breaches.

References

[1] Peter Carey, Data Protection, 7 (Fifth Edition,Oxford university press, 2018).

[2] Seth Karnika.(2013). Computer, Internet and New Technology Laws. Lexis Nexis,Butterworth.Haryana.

[3] Rattan Jyoti.(2011). Cyber laws. Bharat Law House Private Limited.New Delhi.

[4] Kamath Nandan,(2012). Law relating to computers Internet and E-commerce. Universal Law Publishing Co. New Delhi. fifth edition.

[5] Sharma Vakul., Information Technology Law and Practices(Second edition, Universal Law Publishing Company Private Limited.,New Delhi.2010).

[6] Gupta and Agrawal, Cyber Laws, (2nd Edition, Primier Publishing Company, Allahabad.2010).

[7] Vishwanathan Aparna, Cyber Law Indian And International Perspectives, (Wadhwa, Nagpur,2012)

[8] Gupta Apar, Information Technology Act, (2nd Edition, Butterworth, Wadhwa, 2011).

[9] (2011)4 NUJS L Rev 567

[10] (2012) PL February S-2

[11] Ahmad Farooq.(2005).Cyber Law. New Era Publication, Delhi, second edition

[12] Asian School of cyber laws, Cyber Crime and Digital Evidence-Indian Perspective

[13] http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[14] http: //www.cs.cmu.edu/ponguru/iaap