Data Protection and Right to Privacy: Issues and Challenges in India

Kalpana V. Jawale
Assistant Professor, Post Graduate Teaching Department of Law, Sant Gadge Baba Amravati University, Amravati, Maharashtra, India

Abstract

In this article the researcher has tried to discuss data protection and right to privacy: Issues and challenges in India. Data Protection and right to privacy are correlated to each other. Data Protection refers to the set of privacy laws, policies and procedures that aim to minimize infringement right to privacy caused by the collection, storage and dissemination of personal data. Personal data generally refers to the information or data which relate to a person who can be identified from that information or data whether collected by any Government or any private organization or an agency. Right to privacy is a fundamental right under the Constitution of India.

In the current scenario the data protection provisions do not extend beyond the territories of India. Within the territory of India, Sections 43A and 72A of the Information Technology Act provides protection for data. Even data which is outsourced to India gets protection under these Sections. However, when data is sent outside the territories of India, one cannot seek protection under these Sections. India has no jurisdiction in such cases and there is no obligation cast on the countries to which India sends sensitive personal information for processing to have an acceptable data protection mechanism.

KEYWORDS: Data Protection, Right to Privacy, issues, challenges, information Technology Act.

Data Protection and Right to Privacy: Issues and Challenges in India

Introduction:

Data protection law in India is currently facing many problems due absence of proper legislative framework. The Information Technology Amendment Act, 2008 has adopted principles of privacy but the lacuna of data protection laws in the country. The provisions are however not adequate to meet the needs of corporate India. In India companies in the information technology and business process outsourcing sectors handling and accessing all kinds of personal data of individuals. Data information including their credit card details, financial information and personal information also. These types of offences have been covered under cyber crime and infringement of right to privacy. In this article the researcher has tried to highlight issues and challenges regarding data protection and right to privacy in India.

Data Protection and right to privacy are correlated to each other. Data Protection refers to the set of privacy laws, policies and procedures that aim to minimize infringement right to privacy caused by the collection, storage and dissemination of personal data. Personal data generally refers to the information or data which relate to a person who can be identified from that information or data whether collected by any Government or any private organization or an agency. Right to privacy is a fundamental right under the Constitution of India.

The data protection legislations have been developed with Information Technology. Processing of individuals data is an essential part of business in modern India. By way of data processing it is possible to make transaction of buying selling of goods, information to consumers and customers. However offences relating to data theft, misuse private and personal data are increasing in India. In the absence of specific legislation, data protection in India has been enforced of privacy and property rights. Privacy rights are enforced under the Constitution of India and the Information Technology Act, 2008, whereas property rights have been enforced under the Indian Contract Act, 1872, the Copyright Act, 1957, and the Indian Penal Code, 1860.

Under information Technology data is defined as "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 in the memory of the computer"[1].

It means that if there is any misuse of personal and private data is nothing but violation of fundamental right like right to privacy. The IT Act doesn't provide for any definition of personal data. Furthermore, the definition of "data" would be more relevant in the field of cybercrime. Some sections of those Chapters are viewed in India as the "backbone" of the data protection regime. A discussion on these provisions follows.

Research Methodology:

Research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically. In it we study the various steps that are generally adopted by a researcher in studying his research problem along with the logic behind them. It is necessary for the researcher to know not only the research methods/techniques but also the methodology. Researchers also need to understand the assumptions underlying various techniques and they need to know the criteria by which they can decide that certain techniques and procedures will be applicable to certain problems and others will not. All this means that it is necessary for the researcher to design his methodology for his problem as the same may differ from problem to problem. While writing this article the researcher has adopted doctrinal method and collected data from various books of imminent authors, journal and websites.

Objectives: while doing this research the researcher has framed following objectives-

1. To find out relation between right to privacy and data protection In India.
2. To highlight the provisions of data protection under Information Technology Act, 2008.
3. To emphasize issues and challenges regarding data protection in India.

Provisions under Information Technology Act, 2008 regarding data Protection:

Information Technology Act provides civil and criminal liability for a number of specifically proscribed activities involving use of a computer many of which impinge on right to privacy directly or indirectly. Following are some sections or provisions regarding data protection and punishment for violation of rights.

Penalty for damage computer system etc[2]:

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

This section foresees civil liability in case of data, computer database theft and may cover computer trespass, unauthorised digital copying, downloading and extraction of data, computer database or information, theft of data held or stored in media is covered, unauthorised transmission of data or programme residing within a computer, computer system or computer network, use of cookies, spyware, or digital profiling are not legally permissible, unauthorised access to computer data/databases, etc. Hence this section ignores the need to check the liability caused due to loss of computer data, database theft, unauthorised digital copying, downloading, and extracting and transmitting the data, using the cookies etc. The purpose of section 43 (a) is not bounded to unauthorized access gained remotely through a network. It applies also to unauthorized access made physically.

The definition of Section 43A[3] uses the term 'body corporate' which means that the body corporate includes a company, a firm, sole proprietorship, associations and Organisations engaged in commercial prospective. The term used as the 'reasonable security practices and Procedures' include the protection and security aspects and procedures which are desired to achieve the protection of the data caused due to unauthorised modification and use of data which may lead to tampering with the confidential data. This can be specified either as: In an agreement between the parties that is the party holding the data and the party whose is the owner of the data. In absence of an agreement then both the parties have to follow the law prescribed by the government.[4]

This clearly specifies that the contracting parties can Specify in their contract the level of security they want from their disclosing parties if any data loss or damage or data breach has taken place and that the disclosing parties are liable to pay for the damages. Although the amendment act does not specify the meaning of 'sensitive personal data' and states that it means some personal information definition may be included by the union government after consulting the professional and business associations.

Tampering with computer source documents[5]:

This Section states that, 'Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or

alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Under this Act "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form. This section protects computer code source.

Hacking with Computer System[6]:

This Section states that:

- Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.
- Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

This section species the law relating to hacking and is quoted as data protection provision in India. If there is important data stored on the computer which has a value/utility and is to be treated as confidential and such data is been accessed by the unauthorised party then the section is applied. For example if a sensitive email is there on a computer and an unauthorized person accesses the document then the confidentiality of the email is lost then in such case the party liable for the loss comes under this provision. For example if any sensitive personal e-mail is saved in a computer and if any person accesses the said document, then the value of the information is completely lost, this will make then party liable under this provision.

Penalty for breach of confidentiality and privacy[7]:

This section states that, Any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

This is the only Section requiring the consent of the concerned person but, given its limited scope, it would be difficult to consider that it could provide a sufficient level of personal data protection. Indeed, this section confines itself to the acts and omissions of those persons, who have been conferred powers under the Act, rules or regulations made there under. These authorities are:

(i) The Controller of Certifying Authorities,
(ii) The Deputy and Assistant Controllers of Certifying Authorities,
(iii)Licensed Certifying Authorities,
(iv)The Adjudicating Officer,
(v) The Presiding Officer of the Cyber Appellate Tribunal,
(vi)The Registrar of the Cyber Appellate Tribunal,
(vii) Network Service Provider, and

(viii) Police Officer (Deputy Superintendent of Police.

Since the Act has only conferred powers to these authorities, the number of 'data controllers' having duties is rather limited. Data Protection refers to the set of privacy laws, policies and procedures that aim to minimize intrusion into ones privacy caused by the collection, storage and dissemination of personal data. Personal data generally refers to the information or data which relate to a person who can be identified from that information or data whether collected by any Government or any private organization or an agency. The Constitution of India does not patently grant the fundamental right to privacy. However, the Courts have read the right to privacy into the other existing fundamental rights, i.e., freedom of speech and expression under Article 19(1) (a) and right to life and personal liberty under Article 21 of the Constitution of India. However, these Fundamental Rights under the Constitution of India are subject to reasonable restrictions given under Article 19(2) of the Constitution that may be imposed by the State.

The Information Technology Act, 2008 deals with the issues relating to payment of compensation and punishment in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data. Under the Information Technology Act, 2008, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances[8].

Under Section 72A of the (Indian) Information Technology Act, 2008, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to INR 5,00,000.

As of now, the issue of data protection is generally governed by the contractual relationship between the parties, and the parties are free to enter into contracts to determine their relationship defining the terms personal data, personal sensitive data, data which may not be transferred out of or to India and mode of handling of the same.

It is to be noted that section 69 of the Act, which is an exception to the general rule of maintenance of privacy and secrecy of the information, provides that where the Government is satisfied that it is necessary in the interest of:

- the sovereignty or integrity of India,
- defence of India,
- security of the State,
- friendly relations with foreign States or
- public order or
- for preventing incitement to the commission of any cognizable offence relating to above or
- for investigation of any offence,

It may by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. This section empowers the Government to intercept, monitor or decrypt any information including *information of personal nature* in any computer resource. Where the information is such that it ought to be divulged in public interest, the Government may require disclosure of such information. Information relating to anti-national activities which are against national security, breaches of the law or statutory duty or fraud may come under this category.

Challenges:

Cyber security in India is not upto the mark and is an ignored world. Further, India has no cyber security policy and strategy that can be implemented under any legal framework. Merely mentioning that India has formulated a cyber security strategy or policy is not enough till it has a force of law.

One area that India has not touched at all pertains to enactment of cyber security laws. Till now we have no cyber security laws in India. Of course, one or two vague provisions have been incorporated in the information technology Act, 2000 and amendment Act, 2008 of India that happens to be the sole cyber law of India.

Even the cyber law of India is weak and ineffective in tackling the fast growing cyber crimes in India. Many of the provisions contained in the IT Act have crossed the limits of constitutionality. This has made a dominant part of Indian cyber law unconstitutional. In fact, so bad is the position that a need to repeal the cyber law of India has been felt these days.

Therefore we have neither a policy/strategy for cyber security nor legal framework for its implementation. All we have are uncodified and non implementable words that have no significance and legal value.

India has faced many cyber attacks in past and in present. Many of them were not detected for a very long period of time. Indian websites are regularly defaced by cyber miscreants. Cases of cyber espionage are rampant in India. Sensitive and strategic defence forces and ministries computer systems are frequently breached and sensitive data is occasionally stolen. Further the cyber law of India must also be repealed and a strong and robust law must be enacted that is also constitutionally and legally sound.

Sum up:

The Information Technology Amendment Act, 2008 has addressed the lacuna of data protection laws in the country. The provisions are however not adequate to meet the needs of corporate India. Indian companies in the information technology and business process outsourcing (BPO) sectors handle and have access to all kinds of sensitive and personal data of individuals across the world, including their credit card details, financial information and even their medical history. These companies store confidential data and information in electronic form and this could be vulnerable in the hands of their employees. It is often misused by unscrupulous elements amongst them. There have been instances of security breaches and data leakages in high profile Indian companies. The recent incidents of data thefts in the BPO industry have raised concerns about data privacy. Therefore it is clearly violation of right to privacy ynder the constitution of India. Data is converted into information and information is converted into knowledge. In the cyber world all such information is stored in computers. The information may include financial details, health information,

business proposals, intellectual property and sensitive data. Till recently, there was no specific provision to address the issue of Data Protection. However, the Information Technology Amendment Act 2008, has not provide proper solution to data protection.

References:

1. Section 2 (o) of the Information Technology Act, 2008
2. Section 43 of Information Technology Act, 2008
3. http://www.ijens.org/Vol_11_I_06/112206-7474-IJECS-IJENS.pdf
4. Section 65 Information Technology Act, 2008
5. Section 66 of Information Technology Act, 2008
6. Section 72 of Information Technology Act, 2008
7. For More Detail See section 43A of the Information Technology Act, 2008
8. Vakul Sharma, Information Technology Law and Practice, Universal Law Publishing
9. Apar Gupta Commentary on Information Technology Act: With Rules, Regulations, Orders, Guidelines, and Reports, Lexis Nexis Butterworths Wadhwa Nagpur, 2011
10. Monika Kuschewsky, Data Protection & Privacy: Jurisdictional Comparisons, Sweet & Maxwell, 2012