

AN ANALYSIS OF PERSONAL DATA PROTECTION WITH SPECIAL EMPHASIS ON CURRENT AMENDMENTS AND PRIVACY BILL

VISHALAKSHI SINGH¹

Abstract

With the current trends in Information Technology, it has become very difficult to protect personal data of individuals. To overcome these problems, certain amendments were introduced in the Information Technology Act, 2000 vide amendment 2008. The Information Technology (Reasonable Security Practices and Procedures and sensitive Personal data or information) Rules came into force in 2011 and has provision for three groups- Body Corporate, Information Providers and Government. The new Privacy Bill which is expected to come in force soon will override the Information Technology (Reasonable Security Practices and Procedures and sensitive Personal data or information) Rules, 2011 and will efficiently protect the personal data of individual. This paper is an analysis of Data protection laws in India.

In its first section, this paper examines the concept of data and data protection in India. In the second section, it examines the constitutional provision protecting personal data of individuals as well as the history of Supreme Court litigation pertaining to interpretation of the word 'Right to Privacy'. In the further section, it analyses the current position of law on the personal data protection and the requirement of enacting Privacy Bill.

INTRODUCTION

Data is a wide term which includes both personal aspects of individual and commercial aspects. The personal aspect is dealt under privacy rights whereas the commercial aspect is dealt under proprietary rights. “*Data Protection refers to the set of privacy laws, policies and procedures that aim to minimize intrusion into one's privacy caused by the collection,*

¹ B.A., LL.B. (Hons.), College of Legal Studies, University of Petroleum and Energy Studies, Dehradun

storage and dissemination of personal data.²“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.³”

The advancement in technology and e-commerce has not only made life easier but also has given tremendous increase in cyber-crimes, data-theft, misuse of private and personal information etc. India has witnessed various instances of data theft as stated by cyber protection cells. Therefore, to curb data theft, effective and well- formulated mechanism is required. The concept of Right to Privacy is read by the India courts under Article 19(1)(a) and Article 21 of Constitution of India. However, these rights are subjected to reasonable restrictions given under Article 19(2) of the Constitution. Though India has no express legislation governing data protection or privacy, few provisions in Information Technology Act, 2000; Information Technology (Reasonable Security Practices and Procedures and sensitive Personal data or information) Rules, 2011 and The Personal data (Protection) Bill, 2013 deal with data protection and privacy. A codified law on the subject of data protection is still to be introduced in India.

In 2006, in response to EU Directive and negative Press around data theft in call centres, an amendment to the IT Act was introduced to impose fine on corporates and individuals who fail to adequately safeguard personal information.⁴ In 2011, the Ministry of Communications and Information Technology notified IT (Reasonable Security Practices and Procedures and sensitive Personal data or information) Rules, 2011 and released a Press note stating that the rules are applicable to corporates and individuals in India.⁵ The Outsourcing companies in India were exempted from the provisions of collection and disclosure under the rules. The Personal Data (Protection) Bill, 2013 was passed with the purpose to protect the personal data and information of individuals collected by the corporates for a particular purpose and prevent its misuse and entitle the individual to claim compensation or damages due to disclosure of the personal data or information. The redraft of the Bill extends the Right to

² Vijay Pal Dalmia, *Data Protection Laws in India* available at http://www.vaishlaw.com/article/information_technology_laws/data_protection_laws_in_india.pdf

³ Ibid at Pg- 1

⁴ Adrienne D'LunaDirecto, *Data Protection in India: The legislation of Self- Regulation*, Pg- 17A available at http://lawblogs.northwestern.edu/njilb/wp-content/uploads/2015/03/JDCL_Directo-Final-Read_3.9.15.pdf

⁵ Khaitan and Co., *Data Privacy and protection law in India: Understanding the regime*, available at <http://www.lexology.com/library/detail.aspx?g=5e567142-bd88-4c00-a1ea-71203e02614d>

Privacy to all residents of India in compare to 2011 draft which guaranteed the right only to Citizens of India.⁶ Further, the legal framework is discussed in detail.

RIGHT TO PRIVACY AND DATA PROTECTION

The right to protect privacy of an individual is enumerated in the Universal Declaration of Human Rights, 1948 (UDHR) “*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation Everyone has the right to the protection of the law against such interference or attacks.*”⁷

The principle of Right to Privacy is also contained in International Covenant on Civil and Political Rights, 1976. The requirements under both the International treaty are that the state shall implement certain legislations to protect the right of privacy and attacks o reputation. As India is signatory to both the treaties, it is the mandate duty of India to pass such legislation but still India has not passed any separate and independent legislation dealing with the subject matter.

The Constitution of India does not explicitly guarantee fundamental right to Privacy though Judicial Activism has bought it within the realm of Fundamental rights. Article 21 states “no person shall be deprived of his life or personal liberty except the procedures established by law.” The Supreme Court of India deduced the Rightto Privacy from Article 21 wherein the court held that “personal liberty” means life free from any encroachments that is unsustainable in law. The court in a landmark judgment held that “the concept of liberty in Article 21 was comprehensive enough to include privacy and an unauthorized intrusion in to an individual’s home and thus disturbance caused violates his personal liberty.”⁸ In People’s Union for Civil Liberties (PUCL) v Union of India⁹, the court explained right to privacy to be under Article 21 in consonance with Article 17 of International Covenant on Civil and Political Rights, 1968.¹⁰ The gross violations of the right to privacy encouraged the Judiciary to take a pro-active role in protecting the right and providing the affected person adequate compensation and damages.

⁶ Leaked Privacy Bill: 2014 vs 2011 available at <http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011>

⁷ Article 12 of Universal declaration of Human Rights, 1948 to which India is a signatory.

⁸ Kharak Singh v. state of U.P. AIR 1963 SC1295

⁹(1997) 1 SCC 301

¹⁰ CRID- University of Namur, *First Analysis of the Personal Data protection Law in India*, Pg- 27 available at http://ec.europa.eu/justice/data-protection/document/studies/files/final_report_india_en.pdf

The fundamental rights under constitution can only be evoked against the state or state-owned enterprises and not against a private individual or institution. The interpretation of Article 21 is insufficient to provide adequate protection to the data or information of an individual. New technologies make personal data easily accessible and therefore provide platform for miscreants to steal personal data. Due to increase in transfer of data through multiple technologies, data privacy and protection requires more stringent law on the subject. The concept of right to privacy originated as an independent and distinctive concept in the field of law and has been developed and interpreted by the court on case to case basis. There is no compendious code dealing with the right to privacy and is yet to be evolved.

LEGAL FRAMEWORK

INFORMATION TECHNOLOGY ACT, 2000 (IT ACT)

The legislation dealing with the data protection in India is IT Act. Section 43A was inserted in IT Act by way of amendment in 2006 which states-

*“Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, **not exceeding five crore rupees,¹¹** to the person so affected.”*

The explanation part in section 43A defines sensitive personal data or information as “*such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.*”¹²

A new section was inserted vide amendment in 2008¹³.

Section 72A “*Punishment for Disclosure of information in breach of lawful contract - Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another*

¹¹ Inserted vide amendment in 2008

¹² Explanation-III of section 42A of IT Act (Inserted vide amendment in 2008)

¹³ Section 72A of IT Act

person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both."

The IT Act is not the Act which solely deals with personal data protection. The provisions related to personal data protection has been inserted in the Act vide amendments in 2006 and 2008 in response to EU Directive and negative Press around data theft in call centres. The issue of data protection is generally governed by the contractual relationship between the parties. The parties are free to enter into agreements and determine their relationship but subject to section 43A, 72A and 69 of the IT Act.

Section 69 is an exception to general rule of privacy and secrecy of information.¹⁴ It states that "the Central or State Government or any of its officer authorised by Central or State Government can intercept, monitor or decrypt any information transmitted received or stored through any computer resource in the interest of-

1. Sovereignty or integrity of India,
2. Defense of India,
3. Security of the State,
4. Friendly relations with foreign States or
5. Public order or
6. Preventing incitement to the commission of any cognizable offence relating to above or for
7. Investigation of any offence."

It gives the power to the Central and State Government and agency authorised by them to access information relating to personal in nature also. The government can interfere with the data subject to recording reasons in writing.

Section 72 of IT Act states-

"Breach of confidentiality and privacy - Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers

¹⁴ Supra note 1 at Pg-2

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."

These provisions provide protection against data and privacy rights violations by corporations and private individuals.

INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011 (IT RULES)

After European Union enacted strict and stringent Data protection laws, the Ministry of Communications and Information Technology enacted IT Rules in 2011.¹⁵ The Act contains provisions with respect to three categories- Body Incorporates, government and Information Providers. Through a Press note released in 2011 itself, the Ministry stated clearly that the rules are applicable to both the corporates and the individuals.¹⁶ It was framed under section 43A of IT Act after the amendment in IT Act in 2008. It gives definition of sensitive personal data. It states that "*sensitive personal data includes*¹⁷

- *passwords;*
- *financial information, such as bank account or credit card or debit card or other payment instrument details;*
- *physical, physiological and mental health conditions;*
- *sexual orientation;*
- *medical records and history;*
- *biometric information;*
- *any details relating to the above clauses as provided to a body corporate for provision of services; and*
- *any information received under the above clauses by a body corporate for processing, or which has been stored or processed under lawful contract or otherwise."*

¹⁵ Supra note 3

¹⁶ Supra note 4

¹⁷ Rule 3 of IT Rules

The proviso to this definition clearly states that any information which is freely available or accessible in the public domain or under Right to Information Act, 2005 shall not be considered as sensitive personal data.

The IT Rules define personal information as "*any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.*"¹⁸

No legislation provides definition of personal data except IT rules. Further the IT Rules cast a duty upon the Body Corporate to provide a privacy policy which shall be available on the website of such Body Corporate.¹⁹ The policy shall deal with the personal information and sensitive data including purpose of collection and its usage. The IT Rules moreover deal with the process and procedure that should be adopted by the Body Corporate for collection of the personal information and sensitive data.²⁰ It also states that the Body Corporate cannot retain the information longer than it is lawfully required.²¹ The Body Corporate is also required to seek the consent of the information provider before disclosing it to the third party.²² Exception is given to Government agencies mandated under the law to obtain information related to personal information and sensitive data. The Body Corporate has to comply with reasonable security practices as provided under Rule 8 of the IT Rules.

Therefore, it can be said that the new law is stricter and stringent and in par with EU laws, the Body Corporate has duty to comply with IT Rules and ensure transparency in its new privacy policies.

THE PERSONAL DATA (PROTECTION) BILL, 2013 (PRIVACY BILL)

Considering the fact that the laws were not implemented keeping in mind personal data protection, the Government has therefore proposed to enact specific legislations on Privacy. The Privacy Bill on coming into force will override the IT Rules as it recognises an individual's right to privacy and only exception to which is protection of national integrity or

¹⁸ Rule 2(1)(i) of IT Rules

¹⁹ Rule 4 of IT Rules

²⁰ Rule 5 of IT Rules

²¹ Rule 5(4) of IT Rules

²² Rule 6 of IT Rules

sovereignty, national security, prevention of crime and public order.²³ The Privacy Bill has been re-drafted many times yet not passed into law because of two reasons²⁴-

- 1) “A disagreement between the judiciary and intelligence agencies over whether or not the agencies ought to be under the scrutiny of a competent court with respect to interception of personal data when they deem it necessary.”
- 2) “A debate over the extension of protection granted by the legislation to all residents of the country (as opposed to only the citizens).”

The second issue as per the leaked version of the draft Privacy Bill 2014 that the Department of Personnel and Training, Government of India had drafted seems to be sort out as it is stated that the law will be applicable to the residents also.²⁵ The last draft is not publicly available.

The Privacy Bill is more transparent than the IT Rules. It provides guidelines for lawful processing of personal data by specifically stating that the personal data must be treated in fair and lawful manner.²⁶ Persons involved in data processing shall treat the personal information as confidential and shall not disclose it to the third party.²⁷ The data controller and processor have to maintain the quality and accuracy of the personal data and cast a duty upon them to prevent the personal data from destruction.²⁸ The Privacy Bill also contains a special provision for intelligence organisations. The intelligence organisation shall minimize the number of persons within the intelligence organization to whom it is made available and extent to which personal data can be copied.²⁹ Chapter- IV of Privacy Bill deals with the Data Protection authority. It contains the process of appointment of chairperson and his removal, functions of such authority, the powers of such authority and powers relating to inquiries.

The Privacy Bill was drafted with the purpose of curbing the growth of unbridled surveillance and to provide legal mechanism to protect the privacy of the individual. As per the leaked document relating to new Privacy Bill, 2014 the exemption given to intelligence agencies on

²³ Section 7 of Privacy Bill, 2013

²⁴ Data Protection 2016 available at <http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/india>

²⁵ Supra note 5

²⁶ Section 9 and 10 of Privacy Bill

²⁷ Section 11 of Privacy Bill

²⁸ Section 15 of Privacy Bill

²⁹ Section 17 of Privacy Bill

the reasoning that they would be caught in various litigations would defeat the purpose of the Privacy Bill.³⁰

CONCLUSION

The lack of comprehensive legislation related to Privacy and data protection is in great demand as the foreign companies that are doing business in India are concerned for the transmission of confidential data into the country. The need for the law on data protection is paramount. Though data protection is not specifically mentioned in the statutes still after amendment in 2008 in IT Act and the new privacy bill is a huge step towards privacy norms. The only point to be noticed is that the Bill shall be implemented as soon as possible with proper amendment to the last bill published in Public domain. The Privacy Bill must be enacted with sound and effective provisions to ensure adequate safeguards to the collected data and its usage.

³⁰ An analysis of the new draft privacy bills available at <http://www.medianama.com/2014/03/223-an-analysis-of-the-new-draft-privacy-bill-cis-india/>