

DATA PROTECTION: CONTOURING THE PERSPECTIVES FROM INDIAN CONSTITUTION TO PERSONAL DATA PROTECTION BILL, 2019*

Introduction

Information technology has served various advantages to mankind¹ in the form of

- i. Speedy social interaction;²
- ii. Growth of business;
- iii. Enhancing the educational capacity of youth³ etc.

Additionally, advantages of information and communication technology can also be seen in terms of email (an essential communication tool for individuals as well as for businesses), information (availability of huge amount of information about every subject like law, government services etc.), services (like banking, insurance etc.), e-commerce (sale and purchase over internet), software downloads etc., which serve an ease to the human community in almost all spheres of life.

The easy medium of transferring data and quicker communication under its numerous recompenses has given birth to an innovative form of transactions called 'e-transactions.'⁴ The introduction of electronic transactions has given various options to users for carrying out several activities and tasks over internet.

While e-transactions promotes economic gains, economic development, speedy transactions, and support to businesses and consumers in the era of globalization, liberalization and industrialization, it has brought about some unwanted problems as well. It has led to challenges such as global access to services has created a problem of *lex loci* application of law, thereby bringing many jurisdictional issues, absence of corporeal presence has given birth to fake

* *Directorate of Academics*

Views expressed in the Article does not express the views of the Institute.

¹ Scott et al., *Internet Benefits: Consumer Surplus and Net Neutrality*, Institute of Policy Integrity, New York University School of Law, (2011). (Jan.7, 2013), http://policyintegrity.org/files/publications/Internet_Benefits.pdf; See also, Gary James on *Advantages and Disadvantages of Online Learning*. (Jan. 7, 2013), http://www.leerbeleving.nl/wbts/nieuw_basics/addis.pdf.

² *Through internet, communication is faster and easier in comparison to the traditional means of communication, so people on opposite sides of the world can speak to each other over the internet as if they were speaking in person. Apart from this the internet boosts the spread of culture, since all type of communications are made possible through internet.*

³ Latchman et al., *Information Technology Enhanced Learning in Distance and Conventional Education*, IEEE Transactions on Education, Vol. 42, No. 4 (1999).

⁴ *According to Oxford Dictionary: E-commerce consists of commercial transactions conducted electronically on internet. To simply define e-commerce, it consists of buying and selling of products or services (by businesses and consumers), through an electronic medium such as internet and other computer networks, important is that e-commerce is concluded without any use of paper documents.*

identities, mandatory disclosure of personal information for the completion of e-transactions coupled with easy access to available data on the internet has resulted in high probability of loss of data, spoofing⁵ (identity theft), and violation of data privacy. World Trade Organization in its report on e-transactions in the developing countries clearly mentioned that out of various challenges involved in e-transactions, violation of data privacy and data protection seem to be of utmost significance, as affects the most precious right to privacy of the people whose data is processed during electronic transactions.⁶

This makes an apt case to understand and analyse the significance of data protection and the legal protection available to data and its privacy from the contours of Indian Constitution till the contemporary regulation in Indian jurisdiction.

Data Protection/Data Privacy: Meaning and Significance

Data protection in the information era mainly refers to the protection of personal data involved in electronic transactions. Most of the times the terms privacy protection and data protection overlap each other in information technology enabled society.⁷ Data protection is a protection ensuring the privacy, security and dignity of the individual's information circulated in the electronic transactions. Data protection is a category of privacy protection apparent in the information technology era which demands a specific legal regulation. Under the realm of privacy protection, the data protection right ensures persons a control over the entire data connected to him.⁸

The wide-ranging term privacy can be defined as a right 'to be let alone' but under the perspective of internet enabled transaction right to privacy shall ensure the control over one's information. This 'control theory' was established by Charles Fried in 1990, where the theorist believed that 'privacy is not simply an absence of information about a person in the mind of other rather it is a control that a person exercises over information about himself.'⁹

The privacy rights of individual under the information technology era can be classified under two heads viz i. Personally Identifiable Information¹⁰ and ii. Non-Personally Identifiable Information.¹¹

⁵ In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

⁶ World Trade Organization, *E-Commerce in Developing Countries Opportunities and Challenges for Small and Medium-Sized Enterprises*. (Aug. 20th, 2013), http://www.wto.org/english/res_e/booksp_e/ecom_brochure_e.pdf.

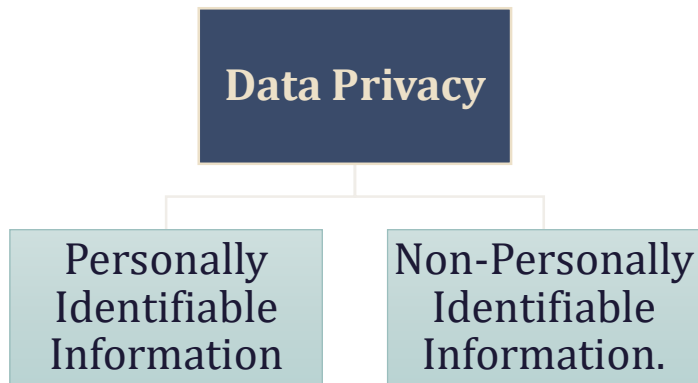
⁷ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Data Privacy refers to the privacy of data involved in electronic transactions. (Sept. 11th 2013), <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>.

⁸ Jori Andras, *Data Protection Law: An Introduction*. (April 4, 2012), www.dataprotection.eu.

⁹ Fried, C., *Privacy: A Rational Context, Computers, Ethics and Society*, New York, Oxford University Press, USA (1990).

¹⁰ Personally Identifiable Information refers to any information that can be used to identify an individual. For example: age, physical address etc. are this type of information which could identify an individual without explicitly disclosing his name.

¹¹ Non-Personally identifiable information includes information like visitors' behavior on website, types of product visited, time of visiting websites etc.



The right to privacy has been designated as a basic right to protect individual's privacy under Article 12 of Universal Declaration of Human Rights, 1948.¹² Article 12 of UDHR reads, 'no one shall be subjected to arbitrary interference with his privacy, family, home and correspondence, or to attacks upon his honor and reputation. Everyone has the right to the

protection of law against such interference or attacks.'¹³

Hence three things are very clear here that a) Right to privacy is recognized as a basic right of an individual, b) it is declared to be protected from unauthorized or arbitrary inference and not against the authorized and logical interference, and c) member signatories have been asked to provide and promote legal protection to right to privacy in their legal administration. Apart from UDHR, right to privacy is also articulated as a human right in the International Covenant on Civil and Political Rights (ICCPR), 1976.¹⁴ It provides that member States are required to adopt the legislative and other relevant procedures to ensure protection to right to privacy against unauthorized inferences and attacks on right to privacy.¹⁵ India being a signatory to this covenant, it is bound to ensure legal provisions to promote privacy protection to its citizen against the unauthorized interferences and attacks to their privacy rights. This includes privacy of offline as well as online transactions.

Although privacy in its literal term can be defined as 'right to be left alone', yet under reference of control theory¹⁶, right to privacy can better be referred as a right to exercise and entertain control over one's personal information in the conduct of e-commerce transactions.

¹² India is a signatory to The Universal Declaration of human Rights 1948. Yearbook of the United Nations 1948-1949, 535.

¹³ The Universal Declaration of Human Rights. (Apr. 3, 2012), <http://www.un.org/en/documents/udhr/>.

¹⁴ Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, w.e.f 23 March 197, Article 49. (Apr. 3, 2012), <http://www2.ohchr.org/english/law/ccpr.htm>.

¹⁵ Article 17, ICCPR: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honor and reputation and 2. Everyone has the right to the protection of the law against such interference or attacks. (Apr. 3, 2012), <http://www2.ohchr.org/english/law/ccpr.htm>.

¹⁶ *Ibid.*

Privacy here can be considered as a set of conditions essential to protect dignity and autonomy of individuals' information transacted in e-commerce.

Data Protection : Legal Perspectives

Information Technology Act, 2000

Individual's data like his name, telephone numbers, profession, family, choices, pan card number, credit card details, social security number etc. are disclosed in the electronic transactions and then are available on various websites.¹⁷ Though the authorized collection and the storage of data may only create probability of the loss of information privacy¹⁸ but the unauthorized access, collection, use, misuse, relocation and transmission of the information to the third party essentially result in the intrusion of information privacy of the individuals. Hence improper control on transmission of information can be the root cause for privacy challenges in electronic transactions. Law will not only determine, what privacy entails, how it is to be valued, and to what extent it should be endowed with legal protection, but also ensures authorized protection to the circumstances under which individuals can value their privacy and protect it from the violation of unauthorized intrusion by others.¹⁹ Knight Bruce in *Prince Albert v Strange*²⁰ upheld that a third party intrusion into one's privacy results in grave violation of right to privacy and hence implies need of legal protection to right to privacy.

To counter the challenges of information and communication technology, the Indian Legislature has enacted Information Technology Act, 2000, Information Technology (Amendment) Act, 2008 and others too, but challenges of information privacy and data privacy are not addressed in an exclusive and specific manner. India is not having a comprehensive legislative framework to deal specifically with privacy issues in electronic transactions.²¹ The Information Technology Act, 2000 was enacted chiefly to facilitate e-commerce; hence privacy is not a prior concern of the Act.²²

¹⁷ Miriam J. Metzger, *Privacy, Trust and Disclosure: Exposing Barriers to Electronic Commerce*, *Journal of Computer Mediated Communication*, Vol. 9 No. 4, (2004). (May 27, 2012), <http://jcmc.indiana.edu/vol9/issue4/metzger.html>.

¹⁸ Information privacy is synonym to data privacy. Information Privacy or data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. (May 27, 2012), http://en.wikipedia.org/wiki/Information_privacy.

¹⁹ Ruth Gavison, *Privacy and the Limits of Law*, *The Yale Law Journal*, Vol. 89, No. 3, 421-471 (Jan. 1980). (May 28, 2012), <http://www.jstor.org/stable/795891?origin=JSTOR-pdf> and.

²⁰ *Prince Albert v Strange* (1848) 2 De G and SM 652, 698; 64 ER 293, 314.

²¹ Shrikant Ardhapurkar et al., *Privacy and Data Protection in Cyberspace in Indian Environment*, *International Journal of Engineering Science and Technology*, Vol. 2, No. 5, 942-951 (2010).

²² Mathur, S. K., *Indian Information Technology Industry: Past, Present and Future A Tool for National Development*, *Journal of Theoretical and Applied Information Technology*. (2006) (Online). (May 28, 2012), <http://perso.univ-rennes1.fr/eric.darmon/floss/papers/MATHUR.pdf>.

Information Technology (Amendment) Act, 2008

Numerous researchers²³ were of the opinion that the Information Technology Act, 2000 in India does not contain sufficient provisions for data protection. The Indian government was aware of the lack of the regulation in this field, but after the analysis of different researches in India and abroad, the Indian Government appointed an Expert Committee²⁴ on Cyber Law to analyze the position of Indian legislation on the protection of personal data and to suggest amendments to the Information Technology Act, 2000.²⁵ The expert committee was formed with the essential objective 'to consider and recommend suitable legislation for data protection (privacy) in the Information Technology Act, 2000.' The Expert Committee in its report²⁶ was of the view that Sections 43, 65, 66 and 72 should be amended for the purpose of 'data protection and privacy.'²⁷

The Information Technology (Amendment) Act, 2008 has been enacted to facilitate and legalize e-commerce transactions, e-fund transfers, e-storage of data, e-filing of documents with the Government departments on one side and to increase the protection of personal data and information for national security, countries' economy, public health and safety on the other.²⁸ Section 43A of this Act directs that all body corporate,²⁹ which are in possession of data and information of their consumers in their computer source, will implement 'reasonable security practices³⁰' to prevent the unauthorized access to the personal data of their consumers. This section further entails that failure to protect the sensitive personal data of the individuals during the processing period by the company will make company liable to compensate the aggrieved person, whose personal data is so compromised.

²³ Jamil and Khan, *Data Protection Act in India Compared to The European Union Countries*, *International Journal of Electrical and Computer Sciences IJECS-IJENS* Vol. 11 No. 06; Parag Diwan and Shammi Kapoor, *Cyber and e-commerce laws*, 4 (2nd ed.2000); Jon Bing, *Data Protection: Jurisdictions and the Choice of Law*; Kuner Christopher, *Data Protection Law and International Jurisdiction on the Internet*, *International Journal of Law and Information Technology*, Vol. 18, Issue 2, 176-193 Oxford University Press.

²⁴ Notification no. 9(16)/2004-EC, January 7, 2005.

²⁵ Nair Latha R, *Does India Needs A Separate Data Protection Law?* *World Data Protection Report*, Vol. 5 No. 12, (2005) (May 29, 2012), <http://www.knspartners.com/files/BNA%20Article-180106.pdf>.

²⁶ Department of Information Technology (August 2005).

²⁷ Blok, P., *Recht on Privacy, Boom (2002)*: In Blok's words privacy can be as: *The individual right to privacy both safeguards an undisturbed private life and offers the individual control over intrusions into his private sphere. Given this definition, the boundaries of the private sphere are central to the meaning of privacy. The right to privacy guarantees individual freedom within the home, within the intimate sphere of family life, and within confidential communication channels. In combination with physical integrity, these 'privacies' form the core of the legally protected private sphere.* (May 26, 2013), <http://www.law.ed.ac.uk/ahrc/script-ed/vol4-4/cuijpers.pdf>.

²⁸ *Workshop Report, National Seminar on Enforcement of Cyber law, New Delhi, (May 8, 2010).* (May 27, 2012) http://catindia.gov.in/pdfFiles/IT_Act_2000_vs_2008.pdf.

²⁹ Section 43 A, Explanation (i) 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

³⁰ Section 43 A, Explanation (ii) 'reasonable security practices and procedures' means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Information Technology Act, 2000 with its Amendment in 2008 does not seem to have an effective address to the concern of data protection and privacy security in the electronic transactions.³¹ After considering an elongated demand from the individuals' to enact a specific legislation to protect their personal information and privacy in electronic transactions, Indian Government has notified the 'Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011' (Here after referred as Rules, 2011) under Section 43A of Information Technology (Amendment) Act, 2008.³² These rules were notified to support and further Section 43A of the Act, for protecting individuals' data in electronic transactions. The aim of these 'Rules', is to provide a strong privacy law for the protection of personal data and privacy in electronic transactions.

Personal Data Protection Bill, 2019³³

The Personal Data Protection Bill, 2019³⁴ was introduced in Lok Sabha by the Minister of Electronics and Information Technology, on December 11, 2019.



Objective of the Bill: The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same.

³¹ Khan M., *Does India have a Data Protection Law?* (Online) Legal Service India. (June 2, 2012), <http://www.legalserviceindia.com/article/l406-Does-India-have-a-Data-Protection-law.html>.

³² *Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Notified by Ministry of Communication and Information technology, Department of Information Technology (11th April, 2011).*


³³ Source: PRS Legislative

³⁴ Detailed Text of the Bill can be accessed at http://prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf


Salient Features of the Bill

- **Applicability:** The Bill governs the processing of personal data by: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India. Personal data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual. The Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator.
- **Obligations of Data Fiduciary:** A data fiduciary is an entity or individual who decides the means and purpose of processing personal data. Such processing will be subject to certain purpose, collection and storage limitations. For instance, personal data can be processed only for specific, clear and lawful purpose. Additionally, all data fiduciaries must undertake certain transparency and accountability measures such as: (i) implementing security safeguards (such as data encryption and preventing misuse of data), and (ii) instituting grievance redressal mechanisms to address complaints of individuals. They must also institute mechanisms for age verification and parental consent when processing sensitive personal data of children.


Decoding the data protection bill

 **WHAT IT MEANS FOR CONSUMERS**

- **DATA** can be processed or shared by any entity only after consent.
- **SAFEGUARDS**, including penalties, introduced to prevent misuse of personal data.
- **ALL** data to be categorized under three heads—general, sensitive and critical.

 **THE GOVERNMENT & REGULATORY ROLE**

- **GOVT** will have the power to obtain any user's non-personal data from companies.
- **THE** bill mandates that all financial and critical data has to be stored in India.
- **SENSITIVE** data has to be stored in India but can be processed outside with consent.

 **WHAT COMPANIES HAVE TO DO**

- **SOCIAL** media firms to formulate a voluntary verification process for users.
- **SHARING** data without consent will entail a fine of ₹15 crore or 4% of global turnover.
- **DATA** breach or inaction will entail a fine of ₹5 crore or 2% of global turnover.

Source: Mint research

- **Rights of the Individual:** The Bill sets out certain rights of the individual (or data principal). These include the right to: (i) obtain confirmation from the fiduciary on whether their personal data has been processed, (ii) seek correction of inaccurate, incomplete, or out-of-date personal data, (iii) have personal data transferred to any other data fiduciary in certain circumstances, and (iv) restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.
- **Grounds for processing Personal Data:** The Bill allows processing of data by fiduciaries only if consent is provided by the individual. However, in certain circumstances, personal data can be processed without consent. These include: (i) if required by the State for providing benefits to the individual, (ii) legal proceedings, (iii) to respond to a medical emergency.

- *Social Media Intermediaries:* The Bill defines these to include intermediaries which enable online interaction between users and allow for sharing of information. All such intermediaries which have users above a notified threshold, and whose actions can impact electoral democracy or public order, have certain obligations, which include providing a voluntary user verification mechanism for users in India.
- *Data Protection Authority:* The Bill sets up a Data Protection Authority which may: (i) take steps to protect interests of individuals, (ii) prevent misuse of personal data, and (iii) ensure compliance with the Bill. It will consist of a chairperson and six members, with at least 10 years' expertise in the field of data protection and information technology. Orders of the Authority can be appealed to an Appellate Tribunal. Appeals from the Tribunal will go to the Supreme Court.
- *Transfer of Data outside India:* Sensitive personal data may be transferred outside India for processing if explicitly consented to by the individual, and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India. Certain personal data notified as critical personal data by the government can only be processed in India.
- *Exemptions:* The central government can exempt any of its agencies from the provisions of the Act: (i) in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, and (ii) for preventing incitement to commission of any cognisable offence (i.e. arrest without warrant) relating to the above matters. Processing of personal data is also exempted from provisions of the Bill for certain other purposes such as: (i) prevention, investigation, or prosecution of any offence, or (ii) personal, domestic, or (iii) journalistic purposes. However, such processing must be for a specific, clear and lawful purpose, with certain security safeguards.
- *Offences:* Offences under the Bill include: (i) processing or transferring personal data in violation of the Bill, punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher, and (ii) failure to conduct a data audit, punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher. Re-identification and processing of de-identified personal data without consent is punishable with imprisonment of up to three years, or fine, or both.
- *Sharing of Non-Personal Data with Government:* The central government may direct data fiduciaries to provide it with any: (i) non-personal data and (ii) anonymised personal data (where it is not possible to identify data principal) for better targeting of services.
- *Amendments to Other laws:* The Bill amends the Information Technology Act, 2000 to delete the provisions related to compensation payable by companies for failure to protect personal data.

Conclusion

Thus the above discussion clearly states that in the newly proposed structure, Personal Data can be kept anywhere, but Sensitive Personal Data can be stored only in India. To be processed anywhere, it is required to be processed with some conditions including consent. Further, Critical Data must be stored/processed only in India.
