Unit 1: Law related to Sensitive Personal Data in India

1

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- What is Sensitive Personal Data or Information
- Procedure to collect the Sensitive Personal Information
- To whom can disclosure of information be made

1.2 INTRODUCTION

The Information Technology Act, 2000 (hereinafter referred to as the IT Act, 2000) isn’t exhaustive and did not specifically deal with the protection of electronic data, until the

Information Technology (Amendment) Act 2008 was passed and the IT Act, 2000 was amended accordingly to include certain provisions relating to electronic data. Further, to give effect to the then brought provision by the 2008 Amendment Act, the Central Government framed certain rules. Hence in the year 2011, the Central Government in exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the IT Act, 2000, passed the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information to deal with personal information and also defined sensitive personal information, with which we are concerned here.[149] These rules are called "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" (hereinafter referred to as the 2011 Rules).

1.3 LEGAL DEFINITION OF 'PERSONAL INFORMATION' AND 'SENSITIVE PERSONAL DATA OR INFORMATION'

The definition of ***"Personal information"*** is found under ***Rule 2(i),*** it has been defined 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 person. It is however different from Sensitive Personal Data or Information. Sensitive Personal Data or Information has been defined under ***Rule 3 of the 2011 Rules.*** It states that in respect of any person, the sensitive data or information is the one which consists of his information relating to:-

i. password;
ii. financial information such as Bank account or credit card or debit card or other payment instrument details ;
iii. physical, physiological and mental health condition;
iv. sexual orientation;
v. medical records and history;
vi. Biometric information;

[149] Tom Gaiety, "Right to Privacy" 12 Harvard Civil Rights Civil Liberties Law Review 233

vii. any detail relating to the above clauses as provided to body corporate for providing service; and

viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

However, by virtue of the proviso to this rule, it excludes from its purview any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force.[150] And thus, this information which is so excluded by virtue of the proviso to Rule 3 isn't considered to be sensitive personal information for the purposes of the 2011 Rules.

1.4 PROCEDURE TO COLLECT THE SENSITIVE PERSONAL INFORMATION

The prerequisites of collecting or obtaining such data or information which has been covered under the definition of the Sensitive Personal Information as per ***Rule 3 of 2011*** Rules have been given under Rule 5 of the same. It includes:

(1) Consent

No Sensitive Personal Data or Information is permitted to be collected without the consent of the person whose information is being sought to be collected. Further, to ensure that this aspect of consent is well adhered to, the 2011 Rules provide that such consent by the provider must be in writing through letter or Fax or can be sent by email and the point worth noting is that the consent here is regarding the purpose of usage of such information. This consent is required before the collection of such Sensitive Personal Information or Data.

(2) Collection of Data must be necessary and for a lawful purpose

The 2011 Rules do permit the individual or entity to collect any information which would be covered under Rule 3 as Sensitive Personal Information or Data only when these 2 conditions are met:

(a) that the information which is sought to be collected is for a lawful purpose which is connected with any of his or its function or activity which in turn is also lawful; and

[150] Samuel Warren & Louis D Brandeis, "The Right to Privacy" Harvard Law Review 193 (1980)

(b) that collecting such sensitive personal data or information is necessary for that lawful purpose.

(3) Knowledge of the person giving the concerned information

The person or entity who is collecting information has to make sure:

(a) that the person whose information is being collected knows that such information is being collected;

(b) that the person whose information is being sought is aware of the purpose for which the concerned information has been collected;

(c) that such person is aware of the person/authority/institution who are likely to be the recipients of the information which is being sought from him;

(d) that such person knows certain details of the agency which is collecting such information as well as the one who will retain such information. Such information shall comprise of the names and addresses of the above-mentioned agencies.

And the person or entity seeking such sensitive personal information must take such reasonable steps as it deems fit and necessary to fulfil the conditions mentioned above.

(4) Also, the person or entity who is collecting the sensitive personal information is under an obligation to provide the person, from whose such information is sought, an option to not provide (or in other words, decline) whatever data or information which was sought to be collected. Discharge of this obligation has to be done by the concerned person or entity prior to collecting such data or information. It is worth noting here that this protection is available to all types of Personal Information, as covered by the 2011 Rules, and hence is also available to information or data other than that covered under sensitive personal data or information at par with the one which is so covered.[151]

(5) Withdrawal of Consent

Along with the prior mentioned right, the person from whom the information is sought also has the right to withdraw his consent which was earlier given. As a safeguard and to ensure that no

[151] Alan F Westin, "Science, Privacy and Freedom" 66 Columbia Law Review 1003 (1966)

one except the concerned person is withdrawing such consent, this withdrawal of consent id also required to be sent in writing.

(6) Information not to be retained for more than required time

Any person or entity who was retaining Sensitive Personal Data or Information is not permitted to retain such data or information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(7) Authorized Use of the Data or Information

As per the 2011 Rules, the information which is collected shall be used for only the purpose for which it has been collected and not otherwise.

(8) Permitting the Correction as well as Amended of the already provided information

Entity or the concerned person shall permit the persons by whom information was provided to review the information they had provided, as and when requested by them and shall ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible.

(9) Keeping the Information secure in compliance with the 2011 Rules

Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

1.5 DISCLOSURE OF THE SENSITIVE PERSONAL INFORMATION OR DATA

The 2011 Rules under Rule 6 covers or encapsulates 3 methods whereby the disclosure of the Sensitive Personal Information is permitted, which will be discussed. As a caution, it is not to be confused with the "transfer of information' which is a different concept and will be addressed in the next heading. The 3 methods by which disclosure is permitted are :

(i) Disclosure to the third party by Prior Permission of the person who gave such information ;

(ii) Disclosure of Information to Government Agencies on certain grounds ;

(iii) Disclosure to the third party in compliance with an order passed under any law in force for the time being.

- ***By Prior Permission***

The Sensitive Personal Data or Information can be disclosed to any third party, provided that the person who has given such information has given his permission for such purpose. Such permission is not mandatorily required, for disclosing such information to the third party, if the information was shared under some sort of contract and that contract itself mentions that the parties agree to disclose such information. Another instance where such permission of the provider is not required is when the concerned person or the entity is under a legal obligation to do so.[152]

- ***Disclosure to Government Agencies***

Rule 6 of 2011 Rules provide certain situations wherein the Sensitive Personal Data or Information shall be shared with Government Agencies, even without asking for the permission of the provider of such information. The contingencies or situations under which the Government Agencies can obtain such data or information are:-

- for the purpose of verification of identity or
- for prevention, detection, investigation including cyber incidents or
- prosecution or
- Punishment of offences

Similar to this Rule 6 of 2011 Rules, Section 69 of the Information Technology Act, 2000, empowers the Central Government, State Government, and the persons specially authorized by Central or State Government in this behalf, to pass an order directing 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, on any of the following grounds: -

- in the interest of the sovereignty or integrity of India ; or
- defense of India ; or

[152] Shrikant, Ardhapurkar & Srivastava, & Tanu, & Swati, Sharma & chaurasiya, Mr & Vaish, Abhishek. (2010). Privacy and Data Protection in Cyberspace in Indian Environment. International Journal of Engineering Science and Technology 2

- security of the State ; or
- 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

- ***Disclosure to the third party under any law***

Rule 6 mentions that any Sensitive Personal Data or Information shall be disclosed to any third party by an order under the law for the time being in force.

1.6 TRANSFER OF INFORMATION

As mentioned above the disclosure of information is different from the transfer of information. In short, where disclosure is usually made to any person or entity which is independent from the one, the transfer is usually used when the information is exchanged between organizations or persons which are connected in a certain way.[153] Rule 7 of 2011 Rules, permits entity or authorized persons to transfer Sensitive Personal Data or Information, to any other body corporate or a person in India, or located in any other country, provided such intended recipient ensures the same level of data protection as provided for under the 2011 Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

1.7 FAILURE TO COMPLY WITH THE PROVISIONS

Since, 2011 Rules draw its powers from the IT Act 2000, there are certain provisions which provide for the contravention of certain provisions, and thus needs to be read for a better understanding of the concept at this point.[154]

[153] Privacy-Enhancing Technologies—approaches and development <http://www.sciencedirect.com/>
[154] Philip E. Agre, Marc RotenbergTechnology and privacy: the new landscape

Section 72A of the IT Act, 2000 provides punishment for disclosure of information, knowingly and intentionally, without the consent of the person to whom the information relates, and in breach of the lawful contract as imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

Further ***Section 43A of the IT Act,*** relates to Compensation for failure to protect data. This provision applies to those body corporate which possess, deal or handle any Sensitive Personal Data or Information in a computer resource which it owns, controls or operates, and is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person. The provision provides that in the situation mentioned above, such body corporate shall be liable to pay damages by way of compensation to the person who is so affected.

1.8 POINTS TO BE PONDERED UPON

In the definition of Sensitive Personal Information under Rule 3 of 2011 Rules, certain information hasn't found a place which by their very nature are sensitive and needs to be adequately protected, and at par with information which has already been given security. In the last few years, reliance on the internet has increased rapidly at an exorbitant rate, and people who use internet usually put certain information which are sensitive but aren't protected by any legal frameworks from being misused.[155] Further, more and more people are joining and regularly using social networking websites, and are readily using electronic communication to be in touch with others. Thus, it is time to give a serious thought about whether electronic communication records including emails, chat logs and other communications made using a computer do not need to legally protected against any possible misuse.

1.9 RECENT LEGAL UPDATES

The Hon'ble Supreme Court of India by its judgment in the case of ***Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors (W.P. (Civil) No. 494 of 2012),*** recognized and

<http://books.google.co.in/books?id=H2KB2DK4w78C&printsec=frontcover&dq=technology+and+privacy&source=bl&ots=1UZmu8TrQp&sig=YJJNgSU61_nTcL_CnCl7Je2LcrQ&hl=en&ei=7L2YS_T2KYSysgOygbnCAQ&sa=X&oi=book_result&ct=result&resnu m=2&ved=0CAkQ6AEwAQ#v=onepage&q=&f=false>

[155] Data Protection Act 1998: 1998 CHAPTER29
<http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1>

pronounced the right to privacy as a fundamental right which is given under the Constitution of India. This landmark judgment definitely calls for an update of the Indian Laws in respect of the Information Technology as well.[156] To achieve this, Personal Data Protection Bill, 2018 was drafted and it is likely to be placed in the upcoming session of the Parliament by the Ministry of Electronics and Information Technology. The Bill intends to regulate the processing of personal data of individuals by government and private entities which are incorporated in India as well as those which are incorporated abroad. The Personal Data Protection Bill 2018, needs to address a lot of things which yet have not been discussed from a legal viewpoint and have been overlooked by the laws which have been in force till now. In the recent updates also, there has been news of government asking certain messaging apps like ***'Whatsapp'*** to share the data with the government authorities. It seems fair from one point, but on the other hand if we look at it from an individual's point of view, the invasion and sharing of chat details of an individual with anyone against or without his consent seems to be in direct conflict with his right to privacy, which as mentioned has been accorded the status of Fundamental Rights. Thus, the least we may expect of the Personal Data Protection Bill, 2018 is to address the issues and conflicts which have already arisen. The Bill in whatever manner passed will have a very big impact on the Information Technology in the upcoming years, and thus should also be far-sighted.

1.10 LET'S SUM UP

In this chapter, we have studied what is Sensitive personal data or information and personal information along with its legal definition. Furthermore, we studied the procedure to collect sensitive personal information and to whom the information has to be disclosed. Finally, we have ended our discussion with the recent legal updates with respect to sensitive personal data or information.

1.11 FURTHER READING

- Ijlljs.in (2019), http://ijlljs.in/wpcontent/uploads/2017/02/AN_ANALYSIS_OF_PERSONAL_DATA_P

[156] White Paper on Privacy Protection in India (Vakul Sharma) <http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf>

ROTECTION_WITH_SPECIAL_EMPHASIS_ON_CURRENT_AMENDMENTS_AND_PRIVACY_BILL.pdf (last visited Nov 20, 2019).

- Elplaw.in (2019), https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf (last visited Nov 20, 2019).
- Webfoundation.org (2019), http://webfoundation.org/docs/2017/07/PersonalData_Report_WF.pdf (last visited Nov 20, 2019).
- Induslaw.com (2019), https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf (last visited Nov 20, 2019).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Define Personal Information?**

The definition of ***"Personal information"*** is found under ***Rule 2(i),*** it has been defined 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 person.

2. **Define Sensitive Personal Data or Information?**

Sensitive Personal Data or Information has been defined under ***Rule 3 of the 2011 Rules.*** It states that in respect of any person, the sensitive data or information is the one which consists of his information relating to:-

i. password;
ii. financial information such as Bank account or credit card or debit card or other payment instrument details ;
iii. physical, physiological and mental health condition;
iv. sexual orientation;
v. medical records and history;
vi. Biometric information;
vii. any detail relating to the above clauses as provided to body corporate for providing service; and

viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

3. What is the punishment for failure to comply with the provisions related to disclosure of information?

Section 72A of the IT Act, 2000 provides punishment for disclosure of information, knowingly and intentionally, without the consent of the person to whom the information relates, and in breach of the lawful contract as imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

4. What is recent case law with respect to the right to privacy?

The Hon'ble Supreme Court of India by its judgment in the case of ***Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors (W.P. (Civil) No. 494 of 2012),*** recognized and pronounced the right to privacy as a fundamental right which is given under the Constitution of India.

1.13 ACTIVITY

Elaborate the procedure to collect Sensitive personal data or information and to whom the information must be disclosure along with the recent cases with respect to privacy issues? (1000-1500 words)