International Journal of Research in Social Sciences
Vol. 8 Issue 12, December 2018,
ISSN: 2249-2496 Impact Factor: 7.081
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Data Privacy And Its Legal Protection In India: A Critique

Ankit Raj Rajial
Ph.D. Research scholar
HPU, Deptt. Of Laws

INTRODUCTION

The digital revolution has changed the methods of information sharing throughout the world. The development of internet and its penetration into the lives of people has made the life easier. Further, with the increasing penetration of mobile phones internet has become an indispensable thing for the modern life. People while using these devices connected through internet are leaving their digital footprints in the form of user data. The Internet of Things (IoT) has further accentuated the generation of data in large quantities. The browsing data of an individual is his own created and has his privacy implications associated with it. Mobile penetration in India is to reach 562 million by the end of 2019. These mobile phone and computers are generating trillions of data every day. This data in turn is being used by the corporates to profile the individuals. We are slowly moving towards an Orwellian state where big brother is having a secret eye on each and every thought and action of ours. After the Supreme Court of India bringing the privacy at the altar of constitutional protection, the data privacy has assumed more significance in current scenario. This data generated online has come to be referred as the new oil of the twenty first century. Considering the value of this new oil, the countries worldwide have begun to provide for legal regulations to tap this new resource. However, the Indian law on the data protection is bit slow to respond than the rest of the world. This paper discusses the Indian law on the data privacy.

DATA MEANING

Data generally means information or facts relating to something or someone. It is a kind of specific information which can lead to identification or profiling of a person. Itmeans "*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 internally in the memory of the computer;"[1]

LAW ON DATA PROTECTION

There is dearth of specific and categorical law on data protection in India. No statute is there in India which specifically target the issue of data privacy in India. India is currently lacking in this aspect. the need for a strong data protection regime is so urgent that the same echoes in the judgment of Hon'ble Justice D Y Chandrachud in the historic Puttaswamy Judgment[2]. Justice Chandrachud pressed the need for having a robust and strong data protection law in India so as to bring India at par with the rest of world in data protection[3]. Currently there is one legislation which to some extent deals with the issue of data protection in India. This is the information and Technology Act, 2000. Beside it there are also the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.[4] Besides these rules there are other rule and guidelines on data protection scattered over RBI Act and TRAI Guidelines.

1. The information and Technology Act, 2000.

This act was in response to the obligation of India under International law to abide by the model law on electronic commerce adopted by the United nation commission on international trade law. Under the Indian Constitution the parliament have power to legislate for giving effect to any international agreement or convention[5]. In exercise of this power the parliament of India enacted the information and technology act in India. The act was intended to streamline the Indian law on e-commerce with the UNCITRAL model law on e-commerce. The provision of the Act dealing with dataprotection are as follows-

1. *Definitions*.

   The Act defines the word Data as a representation of information, facts, concepts etc. which are prepared or are to prepared in a formalised manner and are to be processed in a computer system. This definition includes in its ambit the information stored in modern storing devices like magnetic tapes and hard disks.

[1] Section 2 (o), IT Act, 2000. No. 21, Acts of Parliament, 2000 (India).
[2] (2017) 10 SCC 1.
[3] Id. at 254 (para 180).
[4] Issued by ministry of communication and technology, India on 11 April 2011.
[5] INDIA CONSTI. art. 253.

2. *Compensation for failure to protect data*.

   This section provides for the penalty to a body corporate which fails to protect the data of a person (whose data it holds in its computer system). The scheme of the act mandates the body corporate dealing with sensitive data and personal information to implement and maintain the reasonable security practices and procedures in relation to data and sensitive personal information. Where the negligence of company causes wrongful loss or wrongful gain to anyone, such body corporate is liable to pay compensation by way of damages to such person.

3. *Interception of information*.

   The central and state government has got the power to order for the interception or decryption or monitoring of information transmitted, generated or received through a computer resource. The government can use this power to decrypt data passing,generated,stored inany computer (including mobile phones). However, such power can be exercised by the government on its satisfaction by 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. Further the order of the government must be reasoned and in writing. On the basis of such order the government can order any of its agency to decrypt, intercept or monitor the information or data in a computer.

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

These rules were issued by the central government pursuant to power delegated to it in this regard under section 43A of the Act[6]. These rules define certain important terms viz. -

a) *Biometrics*- It has been defined to mean those technologies which are capable of measuring and analyzing human body characteristics like fingerprints, eye retina iris voice patterns facial patterns DNA etc. for the purpose of authentication. Thus this definition would embrace the modern technologies like finger printer sensors installed on mobile phones, facial recognition and voice pattern recognition used in mobile phones.

b) *Personal information*- This definition is applicable only in respect of a natural person and not a juristic person. Any information relating to a natural person

[6] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

capable of identifying such natural person in combination with other information available with a body corporate.

These rules also categories the sensitive personal data or information which needs protection from illegal disclosure. It is defined to include passwords, financial information like bank accounts, debit or credit cards etc. other kind of information like information relating to physical and mental health condition, sexual orientation, medical records, biometric information etc. an exemption in favour of information provided under the right to information Act 2005 has been provided in these rules.

c) *Privacy policy-* the rules mandates a body corporate receiving or processing Information to provide for a clear and end effective privacy policy for handling or dealing with personal information including sensitive personal data or information. Such privacy policy drafted by the body corporate must always be available for the providers of the information and must be on its website. The policy must state the type of personal or sensitive information being collected. The purpose of collection and usage of such information must also be disclosed in such policy.

d) *Collection of information*- the rules provide for the mandatory written consent of the information provider for providing sensitive personal data or information regarding purpose of usage prior to collection of such information. The body corporate is prohibited from collecting sensitive personal data or information unless such collection isnecessary and for lawful purpose in consonance with the activities and objectives of the corporate. The body corporate shall take steps to ensure that the information provider having the necessary information about the fact that information is being collected and the purpose of collection and the intended recipients of such information.

e) *Time limit*- the rules mandate that the data collected is retained only for the time for which it is required and no further[7].

f) *Withdrawal of consent*- a starking feature of these rules is that the information provider is at liberty to withdraw his consent at any stage after submitting his data to body corporate[8]. The data provider is given the full authority to revoke his consent given for collection of sensitive personal information and data. However,

[7]Rule 5(4)
[8] Rule 5(7)

the data collector can devoid the information provider of the service for which the data was collected. This, sadly, will force the information provider to not to withdraw his consent.

g) *Disclosure of information*- the body corporate is casted with the duty to not to disclose any sensitive personal information and data of the information provider to third party except by his consent[9]. However, if the consent of information provider is already taken for such transfer at the time of acceptance of terms and conditions (as is the case with most of the android and I-phone apps), no subsequent consent is required. An exception is also carved out in respect of information required by the state for maintenance of law and order and prevention of commission of offences etc.

h) *Transfer of information*- the body corporate can transfer the information to those entities, Indian as well Foreign, which follow these rules on data protection of IT Act,2000[10].

i) *Reasonable Security Practices and Procedures* —the body corporates are mandated to follow the reasonable security practices and procedures for data protection. The International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such listed practice to be followed by the body corporate collecting personal information and data.

Conclusion

As mentioned earlier Indians are very rapidly adapting to the mobile phones and other allied technologies based on internet. Mobile phone and internet have become the synonym with the yesteryear requirements of *Roti* (bread) *Kapda* (cloth) and *Maqaan* (shelter). A vast amount of data is being generated each minute by the users of these technology in India. this is also a fact that most of the Indian population is illiterate and lives in villages and semi urban localities. They are unaware about the dangers associated with the profiling based on data generated online. Further aggravating fact is the lack of a comprehensive legislation on data protection in India. there is a limited protection to the data and personal information in the form of rules and guidelines discussed above. These rules and guidelines

[9] Rule 6.
[10] Rule 7.

are not effective to cater to the demands of data protection in modern times. These rules are too broad in language and are lacking in effectively protecting interest of people. The other allied rights of right to privacy like right to be forgotten, right to erasure, principle of data minimization are needed to be protected by the legislature backed laws. There is a need of the hour to frame a comprehensive legislation at par with the international standards of data protection. It is high time that the