# Chapter Seven

# Conclusion and Suggestions

| |
|---|
| **7.1 Conclusion** |
| **7.2 Findings** |
| 7.2.1 Protection of Privacy : Serious Issue |
| 7.2.2 Informational Privacy : Major Dimension of Right to Privacy |
| 7.2.3 Specific Data Protection Legislation: Pressing Need |
| 7.2.4 Health Data: No specific Protection |
| 7.2.5Lack of certainty in Protection of Right to Privacy |
| 7.2.6 Lack of Awareness: An Impediment |
| **7.3 Suggestions** |

## 7.1 Conclusion

The internet is unique medium to exchange of information. The benefits of these technologies cannot be denied. But unrestrained use of it may harm the individual more. In this cyber society, any information of an individual can be converted in to identifiable information of him. Common person approach courts for protection from the invasion on and breach of their privacy which is committed by processing of personal data, by any entity including government.

Hence, in this research work, the researcher intended to study the right to privacy with reference to Information Technology Act, 2000. This research was done with following objectives-

1. To analyse the privacy bills and data protection bills towards protecting the right to privacy.
2. To identify the preventive measures of infringement of interests and rights of persons.
3. To identify global issues and challenges particularly in countries like United States of America., U.K, and
   European Union and also national policy in Cyber Laws.
4. To study the opinion of the stake holders.
5. To examine the role of judiciary in protecting the right to privacy of
   individuals with reference to IT Act, 2000.

## 7.2 Findings

The researcher, to achieve the above-mentioned objectives of study divided the study into Seven Chapters. The First Chapter is of Introduction wherein the Researcher apart from the defining the Objectives and formulating the Hypothesis has done an extensive literature review.

### 7.2.1 Protection of Privacy: A Serious Issue

The researcher studied the use of computers and information technology in various fields of society operations from education to health to defence and control in **Chapter Two -Computer Transactions and Right to Privacy: An Overview.** The researcher made an attempt in this chapter to represent fields in which computer and information technology is used and the instances of

violation of Right to Privacy while using them. The Researcher has also discussed some of the crimes which result in loss of privacy in any one or more aspects. The Researcher found that the traditional uses of computer and information technology are diminishing very fast. The cognitive functions in decision making which made the human being distinct and incomparable are intended to be replaced by new inventions in science and technology. The privacy threats which may result from the use of such technology which is used in IoT, Machine Learning, Data mining and Artificial Intelligence are not visible yet. In this situation, the privacy, security and confidentiality of the personal information or data is very difficult to maintain. On backdrop of this multi-potent technological advancement, the protection of privacy of any person is serious issue faced by the various legal systems.

### 7.2.2 Informational Privacy: Major Dimension of Right to Privacy

Researcher studied the basic meaning, evolution and development of the term and value privacy in **Chapter Three -Right to Privacy: An International Perspective**. In this Chapter the researcher came across the issues and challenges in countries like United States of America, United Kingdom, European Union and India. While studying the historical evolution of the 'privacy', researcher could conclude that 'privacy' is a very fluid value, difficult to define 'Privacy' including all contours of it. It includes mainly in the core, a freedom of human being 'to live alone' i.e. without scrutiny of the society which allows him to develop his personality. Earlier it was associated to tangible right like right to enjoy his property and then evolved and developed to more intangible things like his personal information.

Privacy has many aspects but in modern era of information technology, privacy of personal information has become very important. Personal privacy was encroached by media, first by print media and then by social media through information technology and internet. Loss of control over personal information may result in to loss of his right to decide for himself, his freedom to choose i.e. autonomy which ultimately result in to liberty. A person may lose his other legal rights including fundamental rights. And hence, the researcher found that informational privacy is a major dimension of Right to Privacy.

The researcher, in Chapter **Four** entitled **Right to Privacy and IT Act, 2000: An Interface**, has studied the preventive measures of infringement of interests and rights of persons by examining the legal systems prevalent in modern and technologically developed countries like United States of America, United Kingdom and European Union and India for objective no. 1, 2 and 3.

The researcher studied in detail the laws made in USA-Privacy Act, 1974 and other sector specific privacy and data protection laws, EU-conventions and General Data Protection Regulation, 2018 and UK- Data Protection Act, 2018.

**Privacy legislations in United States**

The researcher concluded that the privacy and protection of data is provided under privacy Act, 1974 and other sector specific legislation is lacking as protection is not available generally. These legislations are applicable to that particular sector. If certain sectors are not protected by specific legislations, the protection is not available to an individual. Moreover each state of United States has its own privacy and data protection legislation. This insufficiency and discrepancy in legislations compromise the privacy and personal data of an individual.

**Privacy legislations in United Kingdom**

For the protection under United Kingdom, the researcher found that United Kingdom has enacted the Data Protection Act, 2018. The impetus is put on protection of personal information. But disclosure of personal information is protected under the breach of confidence as in Douglas. The judgements given by the court show that personal privacy is not provided for. The personal privacy is still protected under tort to property and person or under Human Rights Act, 1992.

**Privacy legislations in European Union**

For the protection of personal information and data, European Union has provided very strong provisions in General Data Protection Regulation, 2016.

**Information Technology Act, 2000: Shortcomings**

Constitution of India does not provide for the right to privacy as fundamental right. Right to privacy was protected by the courts through the judicial creativity holding that this right is covered under Art. 21. In many cases, the Supreme Court, touched the various aspects of right to privacy and upheld this right under the fundamental right governed under Article 21 i.e. Right to Life and several other provisions of the Constitution read with the Directive Principles of the State Policy.

In order to analyse the Privacy Bills and Data Protection Bills and to study their provisions towards protecting the right to privacy, an in - depth study of the Bills was also done. The researcher also studied in detail the Information Technology Act, 2000, and Rules made under the Act.

The researcher analysed the Information Technology Act, 2000, Rules made under it for privacy of personal data or information, 2011, and rules for interception of data by the government, 2009, which are primary legislations. These legislations nowhere expressly and elaborately provided for person's informational privacy and data protection in era of continuously and fast developing technology. This protection is essential for personal, informational and decisional privacy of a person. The researcher has inferred that legislation suffers from the following loopholes:

1. Information Technology Act, 2000 is protecting the provisions regarding privacy of sensitive personal data or information in a limited sense under S. 43A. But the definition of sensitive personal data is not provided under it.
2. The term 'sensitive personal data' is defined in Rule 3 under Information Technology(Reasonable Security Practices And Procedures and Sensitive Personal Data or Information) Rules, 2011, which is delegated legislation for rule making power provided under S. 43A. This means these rules can made or can be amended by the executive officer empowered by Central Government. These rules are not made by Parliament by conducting discussion on the matters. Threat to privacy is more likely when rules are made by delegated/subordinate legislation.

3. Sensitive personal data is to be protected by 'body corporate'. The explanation to S. 43 A provides the definition for 'body corporate' include the firm, company or association engaged in commercial or professional activities. This not applicable to the government as it is not engaged in commercial activities.

4. It covers liability of body corporate only possessing or handling the sensitive personal data or information in negligent way. But there are many other ways and methods by which such data is compromised or misused or abused.

5. Information Technology Act, 2000 and the Rules made under it are not providing for cross-border transfer and processing of data.

6. The government is providing services to citizens through electronic media using information technology. Personal information is also gathered with the government but government's responsibility is nowhere provided.

7. In many situations, government actions are resulting into violation of privacy of person. Information Technology Act, 2000 and Rules made under it do not provide any protection against these actions. Under these legislations, government's liability is not provided for.

8. Responsibility of intermediaries are provided in Information Technology Act, 2000 on open ended terms. Any activity can be covered under it for exclusion of the responsibility. Moreover, the liability of cloud service providers is not provided specifically.

### 7.2.3 Specific Data Protection Legislation: Pressing Need

Privacy Bills in 2011 and 2014 and Personal Data Protection Bills were drafted in 2013, 2018 and 2019, but no legislation is made for protection of privacy and personal data till today. The detailed analysis of the all the Bills introduced till date has been done by the Researcher in Chapter Four. The Privacy Bill, 2019 is the latest on in the series of the various Bills introduced in this context. The position till the submission the present thesis by the Researcher is, that the Bill was presented in Parliament and presently it is sent to Joint Select Committee. Even if it is enacted as an Act these shortcomings which are discussed below are going to affect the right to privacy of an individual.

**Shortcomings of Privacy Bill, 2019**

There are certain loopholes in the provisions.

1. While giving protection for data privacy the processing is to be done in 'fair and reasonable way'. But there are absence of guidelines for what is 'fair and reasonable' way. This is important as data fiduciary has to be able to show to Data Protection Authority that data had been processed in a fair and reasonable way. The Standard is to be provided to judge 'fair and reasonable'.

2. Processing of data is permitted without consent in certain situations by state like for provision of services or benefits to data principal. This purpose is ambiguous. Such benefits shall be given without consent for processing. Permission for processing without consent for all services of public functions by state is too wide.

3. They are not applicable to both public and private sectors equally as private sector companies exercising same function have to obtain consent but Public Sector Company does not need.
4. Further, processing without consent is permissible 'for reasonable purposes' also. These 'reasonable purposes' include various parameters. These exemptions from consent requirement may be susceptible to be misused by the government. Such authority may be used for surveillance.
5. Any social media intermediary having users above particular number (the threshold) as notified by Central government as significant data fiduciary whose actions have significant impact on electoral democracy, but definition of 'significant impact' is not provided for deciding the impact is 'significant'.
6. Similarly, another contentious provision is relating to the definition of 'Critical Personal Data', which is not defined under the Bill but the Bill states that it is is to be provided by Central Government . This gives sweeping powers to the Executive. This too appears to be too wide delegation of powers to the Executive. The researcher submits that what amounts to 'Critical Personal Data' must have been defined in the Bill as this can be said to be one of the central definitions in the protection of data.

7. It provides about the power of Central Government to exempt any agency of Government in respect of the processing of the personal data from application of the Act where it is 'necessary or expedient' on the grounds stated in the section. It is possible that this provision, may be misused or abused by the government. The term 'necessary and expedient' gives power to state to form subjective opinion about the threat.
8. The test of proportionality which was provided earlier is dropped.
9. The power to instruct the data fiduciary to hand over non-personal data to government is not very clear. Non-personal data is explained as which is not personal. No other parameter is provided. There is a possibility of threat to right to privacy from the government itself.

**Right to be forgotten:** The unique right which is provided under GDPR is also provided under this Bill in somewhat modified way. This Bill provides for right to be forgotten in different way than GDPR. It provides data principal has right to restrict or prevent continuing disclosure of personal data by data fiduciary related to data principal on certain conditions as data become irrelevant Adjudicating Officer determines its applicability, after considering the conditions in the section and such right can only be exercised if data principal's rights and interests are overriding the right to freedom of speech and expression and right to information of any citizen.[1]

Here authority to decide as to erase the personal data is vested with the Adjudicating Officer and only if data principal's interests are overriding the right to freedom and speech and right to information of others, then he decide to erase the data. But under GDPR, the right cannot be exercised if data processing is necessary under legal obligation, for exercising freedom of expression and information, and for public interest as public health, and other exemptions[2]. No officer is provided to decide the erasure. Only Data Controller has to decide. Under GDPR, the controller, who has made the data public, shall

[1] The Personal Data Protection Bill, 2018, S.27(2),
[2] General Data Protection Regulation, Art. 17

inform the other controllers who are processing the data to erase any link to, or copies or replications of such data[3]. This provision is not included in this Bill.

In business transactions or for employment purposes creditworthiness of the parties is important and essential factor for its successful operation. Electronic media or platform is easily accessible by people in this information technology era. It is easy to verify antecedents of person with whom they are going to deal or to whom they are going to employ. But if the right to be forgotten is provided, there will be a possibility that person committing such offences may repeat it after their repeal from electronic media and persons associated with him later may suffer because of this. There is also a possibility that such action may be repeated again and again. The researcher is of the opinion that such right must not be made available in cases where the person has committed any criminal offence of high gravity and/or heinous offence or offence of moral turpitude. In the Bill, these things are not thought or provided for.

As it is evident from the discussion so far, that there is lack of legislative framework for protection of privacy for the personal information or data generated through internet. There is a need for a specific law dealing with Personal right to privacy by determining the liability of private persons as well as of government and providing remedies for it. Such responsible legal framework is sign of mature and democratic country.

Although, a step in this direction is taken by India; however, it is high time that the Privacy Bill soon becomes a legislation. Although, the researcher argues that the Privacy Bill, 2019 suffers from some drawbacks and still is not at par with GDPR, still, submits that the final enactment of the Bill, clearing all the law making formalities , will be a welcome step; as having a specific data protection legislation , is the pressing need of the present time.

### 7.2.4 Health Data: No specific Protection

[3] General Data Protection Regulation, Recital 66

After globalisation, India has adopted information technology in various fields and it is used by different entities including government. The use of Information Technology in various sectors has been dealt at length by the Researcher in Chapter Two. Submission of personal information is precondition for using computer and internet to get services or information. In this information era, the personal information has become all-important. Information submitted for availing service may be used for any other purpose by the entity to which it is submitted. It is used as raw material to generate more information about the person along with the persons who are in connection with him.

One such example can be of transactions covering health data which are important to be protected as breach and invasion make the individual more vulnerable. The situation becomes more complicated when the doctor is attached to various hospitals and he refer the patient to some other speciality doctor. Medical data of the patient is transferred using information technology to such other hospital, nursing home or any private practitioner whichever the case may be. Such data can be accessed, verified, disseminated by the other hospital, nursing home or any other entity who provides the medical care to the patient. Sharing of data occur between intra and inter hospitals as well as with outside agencies.

If the diagnostics are conducted in the units which are run privately-which is more common in semi urban areas in India or not registered under the proper Act, there is no guarantee of privacy of any sensitive medical data. Chances are high for compromise the privacy and security of data by these privately run medical centres or diagnostic centres which are not registered under proper Acts and also do not conduct diagnostic processes with uniform agreeable standards with proper privacy settings. By the collected datasets, the health care sector detects the trends quickly and target the consumers accurately.

In sensitive personal data also, health data is more important as compromise of which harms the person very gravely. Ministry of Health and Family Welfare enacted the provisions for protection of privacy, confidentiality and integrity of such medical data under Digital Information Security in Healthcare Act, herein

after (DISHA)[4] in 2018. But this draft was given for its inclusion in Data Protection Act which the Ministry of Electronics and Information Technology is drafting to avoid duplicity for protection of personal data in general, as per the press release from the Ministry of Health and Family Welfare.[5] But separate legislation is necessary for protection of health data as data protection law is going to cover many things relating to e-commerce and e-governance.

Further, as stated above, the IT Act, 2000 doesn't define 'sensitive data'. However, it is found that among sensitive personal data, health data has become valuable for the organisations globally. It is transferred to outside countries and needed to be protected by specific legislation. Hence, a need for separate legislation emerges for protection of health data as data protection law is going to cover many things relating to e-commerce and e-governance as well. It is the need of the time that there should be separate sector specific data protection legislation available as Health Insurance Portability and Accountability Act, 1996 (HIPAA) of USA for protection of digital health data in India.

### 7.2.5 Lack of Certainty in Protection of Right to Privacy

The Researcher, in **Chapter Five titled 'Judicial Responses'**, has studied and analysed several judgements in order to determine the actual status of various laws and regulations on privacy protection in India in comparison with the judicial decisions in USA, UK and European Union. The objective of this Chapter was to examine the role of judiciary in protecting the right to privacy of individuals with reference to IT Act, 2000.

The Supreme Court of India was and is providing the protection against the breach of Right to Privacy relating to its various contours. But as there is no separate and specific legislation, the right is protected under Art. 21 Right to life and liberty. There are limitations for the protections provided under Art. 21 as

[4]Available at www.nhp.gov.in/NHPfiles/R_4179_1521627488625_O.pdf ( Last visited on May 24, 2020)
[5] https://pib.gov.in/Pressreleaseshare.aspx?PRID=1578929 ( Last visited on May 24, 2020)

its main purpose is to protect the person against the arbitrary actions by the state. Court has stretched its creativity to maximum. But as the commercial transactions using information technology have increased so much and used by common person as well as by the government, the threats to right to privacy may be more and in unprecedented way. It may happen that the breach of right to data privacy cannot be connected to right to life and liberty. In absence of data protection legislation, there is uncertainty relating to the protection of privacy and protection of data. It is evident from the discussion on judicial response.

The analysis of judgements indicates that even though the Indian courts are in favour of granting relief and justice to common person for encroachment or violations of their right to privacy and data protection, they lack the certainty in absence of the express provisions. This could be seen when the different High Courts were called upon the right to be forgotten. Thus, with Chapters 4 and 5, the researcher achieved objective no. 1, 2, 3and 5 of this research work.

### 7.2.6 Lack of awareness: An impediment for Protection

The researcher had used non-doctrinal method for objective no.4 and to meet this end, the researcher used questionnaire as a research tool, which was filled in by stakeholders belonging to different fields of society like students, teachers, accountants, housewives, police personnel etc. The data collected from One Hundred and fifteen respondents were analysed and interpreted in **Chapter Six: Data Analysis and Data Interpretation** of this research work. The inferences are as follows:

1. The analysis done shows that stakeholders are grossly unaware that personal information/data is important to protect the privacy.
2. Majority stakeholders do not include health information in their personal information. Majority are not aware about the tracking of their browsing history by different websites and companies.
3. Majority of them are not aware that data protection is an element of Privacy and its breach is an offence under IT Act, 2000.
4. Majority do not know when government can access and intercept the data.

5. All of them use social media apps but majority of them are not aware about privacy features of these apps.
6. Considerable number of them believe that police officials are aware about provisions of protection of personal information, but response of the police personnel show that many police officers are not aware about the same.
7. Majority stakeholders are not aware that their personnel information is tracked by organisations.
8. The stake holders use public wi-fi and considerable number of stakeholders are not aware about its privacy issues.
9. From the response of the police personnel, it is also observed that stakeholders answered that all police personnel are not provided the necessary information about laws pertaining to cyber activities. This shows the lack of awareness about the right to privacy relating to personal information.

**Conclusions drawn on Hypothesis**

Lastly on the basis of the above discussion and inferences the researcher has drawn conclusions on Hypothesis of this research work as follows:

**Hypothesis-1.** Is it possible to achieve justice or to prevent failure of justice as there is less sensitivity and political wish to enact law for protection of right to privacy?

The said hypothesis has been affirmed by the inferences drawn in this research study.

**Hypothesis-2** Can a judiciary deliver justice and prevent infringement of the rights, in absence of clear provisions protecting Right to Privacy?

The said hypothesis has been affirmed by the inferences drawn in this research study.

**Hypothesis-3** Does lack of awareness among people about the clear provisions of Information Technology Act, 2000, will result in to infringement of Right to Privacy?

The said hypothesis has been affirmed by the inferences drawn in this research study.

**Hypothesis-4** In absence of the any check on the Government or any other entity for gathering and dissemination of information of a person, is it possible to guard the right of person to his privacy?

The said hypothesis has been affirmed by the inferences drawn in this research study.

**Hypothesis-5** As there is lack of provisions regarding responsibility of intermediaries, service providers, is there a possibility that intermediaries, service providers misuse the power?

The said hypothesis has been affirmed by the inferences drawn in this research study.

### 7.3 Suggestions

1. Like other developed countries as European Union, United States of America, and United Kingdom, India should develop a strong data protection legislation for protection of privacy relating to personal data.
2. Though the Personal Data Protection Bill, 2019 if passed by the Parliament shall give protection of personal data breach, still there is lack of provisions for protection of non-personal data as it is excluded from the protection. With the help of innovative scientific data processing techniques this non-personal data can be applied to identify the person.
3. The government must also be made liable for protection of data and invasion of privacy. In the Personal Data Protection Bill, 2019, exemption is granted to the government relating to many activities.
4. Instead of one general data protection legislation for protection of data against data breach and invasion of privacy in all the sectors, separate legislation must be enacted for sensitive health data. Digital Information Security in Healthcare Act (DISHA) was suggested but it was merged with the Personal Data Protection Bill, 2019 for the fear of duplicity. But invasion and breach of health data makes the individual more vulnerable. Separate legislation as DISHA must be enacted for collection, use, storage, dissemination and transfer of data intra and inter clinical establishments.

4. Liability of cloud service providers must be specifically mentioned. Strict liability must be imposed on the intermediaries and service providers. Responsibility of cloud service providers must be specifically mentioned.

5. While defining the liability, the terms imposing liability must not be open ended but clear and unambiguous.

6. Provisions regulating the power of government to collect data from intermediaries, services providers must be provided in specific way.

7. Under S. 69 of IT Act, 2000, Government's power to intercept the communication must be restricted.

8. There should be specific provisions for control and regulations regarding installation and use of CCTV and biometric data collection devices.

The need for protection of data or information has increased with processing of the data outside country being on progressive path. The Data Protection Laws are still in the making. Apart from a few privacy protections provisions in the IT Act, 2000, the researcher finds a vacuum in the system for the protection of privacy. Hence, it is concluded after foregoing discussion and analysis of data that there is a big privacy threat which has major implications and profound effect on freedoms and liberty of person. India immediately needs strong privacy and data protection legislation on the backdrop of the increased activities on internet and rise in commercial transactions through information technology.