Data Protection Law in India: A Critical Legal Study with Special Reference to Right to Privacy

ABSTRACT

SUBMITTED TO THE
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW

FOR THE AWARD OF THE DEGREE OF

Doctor of Philosophy

IN
LAW

Supervisor
Dr. Pradeep Kumar
Associate Professor

Submitted By
Sharad Kumar Pandey
Enrollment No. 1496/19

DEPARTMENT OF LAW
SCHOOL OF LEGAL STUDIES
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY) (NAAC A++ Accredited)
VIDYA VIHAR, RAEBARELI ROAD, LUCKNOW-226025 (U.P.), INDIA

2023

ABSTRACT

DATA PROTECTION LAW IN INDIA: A CRITICAL LEGAL STUDY WITH SPECIAL REFERENCE TO RIGHT TO PRIVACY

There has been much increase in the proliferation of electronic gadgets and software applications throughout the most recent few years, and there has been a considerable increase in the total amount of data that has been generated. The analysis of what is commonly referred to as big data gives substantial value to today's businesses, and these businesses frequently base their business strategy on the outcomes of such analyses. The question that needs a response is, "Do individuals have any control over how information about them is accessed and processed by others?" Even though there is no room for debate on the effectiveness of this approach from a business perspective, the question that needs to be answered is as follows: "Do individuals have any control over how others process information about them?"

Whatever the number of attributes, layers or clusters that may surround and distinguish the types and levels of privacy, the keystone of the privacy edifice is always the private space around the individual. This space may be small or large, physical or virtual, in the body or mind, mental or emotional; it is this basic space that determines whether or not the individual is at liberty to enjoy his privacy with dignity.

The right to privacy is something that has yet to be established. Individual has the right to demand damages based on tort law if they feel that their privacy has been invaded, which is a concept that originates from common law. One of the first cases on the said topic was *Semayne's* Case.

In this particular instance, the Sheriff of London was required to enter a property to carry out the terms of a legal writ. While acknowledging a man's right to solitude, the legendary judge Sir Edward Coke J. once observed, "The house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose." The idea of personal privacy saw significant growth and development in England during the nineteenth century and is widely accepted in the modern world.

In the case of *Campbell* v. *MGN*, the court decided that if there is an intrusion in a situation where a person can reasonably expect his privacy to be respected, that

intrusion will be capable of giving rise to liability unless the intrusion can be justified. In other words, if there is an intrusion in a situation where a person can reasonably expect his privacy to be respected, then that intrusion will be liable.

The Information Technology Act, 2000 defines data in a very elaborate term. On the other hand, the idea of data is not restricted to information stored in an electronic form; instead, it comprises information stored in a physical form, such as on a piece of paper. For example, data can be saved in both electronic and physical formats.

PRIVACY AND DATA PROTECTION

The emerging era wants to preserve individuality in the digital world. The privacy protects personal liberty, dignity, and independence against intrusion. It involves managing and protecting personal data, choosing its acquisition and use, and maintaining privacy. Privacy protects individuality, liberty, and dignity. Many international and regional human rights instruments consider it a fundamental right, although not all State Constitutions. Privacy safeguards human autonomy, family, lifestyle, and personal choices. Data privacy is the informational protection of personal information. It controls private data collection, storage, usage, and distribution.

People have the right to know what data is collected, how it will be used, and whether to consent or not to such collection and use. Unless with legal permission, it must restrict state or other state machinery for intrusions into houses, including searches, surveillance, and monitoring. Privacy includes communication secrecy. It protects phone conversations, emails, and private messages from eavesdropping.

Encryption, management, biometrics and online privacy are explored. These safeguards protect against unauthorised privacy intrusions. Privacy has certain limitations, which may be justified when mandated by law, necessary for national security, public safety, crime prevention, or protecting rights and freedoms of others. Many Federal Legislations and the Universal Declaration of Human Rights protect privacy. It covers digital society's personal space, liberty, and dignity. Privacy provides independence, grace, and control over personal information and life. It protects democracy, individual freedom, and trust.

In India, there are a variety of laws and regulations that address data privacy and data protection in different segment. There were laws and regulations to

safeguard privacy of persons by preventing unauthorised access to their personal information and requiring responsible data management practices. The following are the most pressing concerns concerning the security of personal data and privacy in India:

Personal Data Protection Bill, 2018: This was in response to the report of the Srikrishna Committee prepared on the direction of the Ministry of Electronics and Communication following the order of *K. S. Puttaswamy* v. *Union of India* judgement**.**

Personal Data Protection Bill, 2019: The Personal Data Protection Bill, 2019 (PDP) is a comprehensive legislation that intends to provide a legal framework for protecting personal data in India. In January 2019, the measure was first prepared for consideration. This bill was withdrawn from the Parliament and presented a new bill in 2022.

Digital Personal Data Protection Bill, 2022: This Bill came to replace the Personal Data Protection Bill 2019. It has been presented in the Parliament but has not passed as a Law. It is again withdrawn from the Parliament.

The Digital Personal Data Protection Act, 2023: This Act has passed by both houses of Parliament in the monsoon session of the year 2023. This has got the assent of the President on August 11, 2023. But it has not been notified. It is published for general information.

Information Technology Act, 2000: The Information Technology Act, 2000 (IT Act) is the most critical legislation that oversees electronic transactions and cyber security in India. It was passed in the year 2000. The year 2000 saw its passage into law. It includes legislation that deals with protecting personal data and penalties for unauthorised access, disclosure, or abuse of data. These laws can be found in the document.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016: It is the piece of legislation that governs the Aadhaar system of identification. It establishes safeguards for the collection, storage, and use of data from Aadhaar to safeguard the right to privacy of individual and ensure the confidentiality of their biometric and demographic information.

Data Localisation: The Reserve Bank of India (RBI) has issued an order mandating that several categories of personally identifiable information obtained by financial

institutions be stored and processed within the country. The term for this practice is ‘data localisation’. This requirement for the localisation of data aims to make it possible to strengthen both the protection of data and the access that Indian authorities have to it.

Certain Industries have their own set of requirements to meet to protect the data of their clients or customers. Numerous sectors, such as banking, healthcare, and telecommunications, each have legislation and norms about the safety of customers personal information. For example, the Health Insurance Portability and Accountability Act (HIPAA), 1996 is the law that governs the protection of healthcare data in the USA, and the Telecom Regulatory Authority of India (TRAI) has released Regulations on the privacy and security of telecom subscriber information. These laws and regulations are in place to ensure that sensitive data is kept private and secure. In addition, both of these organisations ensure that information is kept confidential and protected from unauthorised access.

In general, the Indian data protection standards demand that organisations seek the informed consent of individuals before collecting and processing their data. This consent must be obtained before the data can be collected and processed. In addition, it is anticipated that businesses will give privacy statements that are clear and concise, revealing the intent of the data collection, its scope, and the recipients to whom it is meant to be distributed.

The Information Technology Act mandates all enterprises to immediately notify the Indian Computer Emergency Response Team (CERT-In) of any data breaches or security events and any affected persons, depending on the circumstances. Therefore, business operations in India must stay current on the most recent trends and changes in their respective industries. That is necessary to ensure that client information is kept confidential and that they comply with all applicable rules and regulations.

NEED OF THE STUDY

In the digital era, researcher finds a massive gap in the safety of individuality and secure personal information in this prospect where almost every tip is easy to trace. In this day and age of lightning-fast technological advancement, we are up against the formidable problem of protecting personally identifiable information. Concerns have been raised about the legal framework regulating the operation of data

processing systems in limitless boundaries. This framework is responsible for ensuring that data is handled appropriately.

When technology is everywhere, safeguarding sensitive data is becoming more critical, and hackers are growing more innovative. We live in a time where technology affects practically every aspect of our lives. These are some of the fundamental reasons protecting personal data is crucial in a digitalised society.

Data security is essential in Internet-connected culture of modern times. Individuals must protect their information, which may be Digital personal, financial, and commercial data. Strong encryption, safe storage, and complete cyber security safeguard data from unauthorised access, hacking, and other cyber dangers increased digital privacy issues. Consumers want to control the collection, usage and sharing of data. Data protection rules like the GDPR protect people from these risks in the EU.

Protection from cybercrime needs data security, including data breaches, ransom ware attacks, and identity theft. Businesses may avoid data breaches and cyber-attacks through multifactor authentication, intrusion detection, and employee training. In the digital economy, when data is safe, people are more willing to shop online, exchange personal information, and use digital services. Clients trust that data-protected firms are needed at this time. Governments regulate data protection worldwide to ensure the importance of such data.

Companies must follow GDPR, CCPA, and other industry-specific standards to prevent legal concerns and brand damage. Privacy by design and secure data practises enabling innovation, ethical data-driven methods, and sustainable digital transformation. In conclusion, data protection is essential in to safeguard privacy, prevent cyber-attacks, develop trust, comply with the law, ensure business continuity, and perform ethical obligations. Responsible, productive digital enterprises need data protection to ensure the winning of the trust of their clients.

UTILITY OF THE STUDY

This research would be helpful in creating awareness about the importance of data and its protection. The study would also be helpful to many students, teachers and professionals in having an understanding of this area in a better way. This research would be well-intentioned and would turn out to be beneficial reference material for individuals interested in data protection.

STATEMENT OF PROBLEM

(1) Compulsory disclosure of an Aadhaar number for availing of many government benefits purposes poses a great threat towards the personal information of an individual, which includes his biometric information since this information is very sensitive and crucial because it is saved under the control of the government.

(2) The CoWIN portal data leak provided an opportunity to breach Aadhaar details, biometric details, and port details, which are very serious in nature. At the time of the COVID-19 pandemic, everyone was compelled to provide personal information for vaccination run by the government.

(3) The Aarogya Setu app, which collected the information of the COVID-19 patient for contact tracing, is without any proper legal justification for collecting and utilising all the information from the person.

(4) Facebook data leak is causing an infringement of our basic personal details, mobile numbers and every other detail which has been provided on Facebook by the user in the normal course of business. Facebook is involved in the collection of personal information in the name of basic account information. But this information is used for commercial purposes.

(5) Fake calls using the internet are a problem in day-to-day life without having any background of that call. Nowadays, most of the time, one gets fake calls using internet media. This is because the location of these fake calls is not easy to trace as compared to normal calls.

(6) Spam message is sent through the internet for different types of unlawful activities. These messages are usually used to provide an opportunity for fraudsters to trap the person by accepting their plan. Sometimes, these messages are used for updating the Know Your Customer form. It is a very easy method to commit fraud by entering personal information.

(7) Digital media is the easiest place for committing different types of crime, which can cause harm without the involvement of any human. There is a great threat due to the invasion of cyberspace. Our personal information sometimes, our personal pictures may surface in online mediums without one's information.

(8) The increase in artificial intelligence in every field is a severe compromise towards the security of personal information and other issues. There are many

companies involved in promoting and investing in the creation of different types of artificial intelligence software. They use it as per the requirements of their industry. The use of artificial intelligence may cause a breach of privacy as well as the protection of individual data.

(9) Identity theft is done to commit different types of unlawful activities. It is common nowadays because cybercriminal uses the identity of a different person by hacking or other ways to target the object to complete their criminal activity without fearing law enforcement.

(10) Social networking sites are a place where one's data is collected and used in different ways. Due to the advent of the internet, there are a number of social networks throughout the world. But every social networking site collects the personal information and uses it in their commercial activity and also the promotional activity of the social networking company

(11) WhatsApp privacy policy creates a two-tier norm that is one for the European Union and the other for the rest of the world. WhatsApp has a dual privacy policy because, in the European Union, there is strict compliance with the General Data Protection Regulation, which may impose heavy penalty.

(12) Technology raises privacy concerns which include unauthorised access, surveillance, and monitoring financial privacy of an individual. Due to the increase in technological activity, there is a range of issues involved, like unauthorised surveillance either by private players or sometimes by the state. Pegasus-like spyware, which is made by Israel and sold to different countries, poses a severe threat to compromising personal information which may be found in mobile phones, email or in any other social media place.

(13) The presence of precise legislation is essential in order to validate any infringement upon privacy of an individual, as mandated by Article 21 of the Indian Constitution. In order to avoid every type of intrusion into personal information, there is a need for precise legislation which may be able to deal with every type of intrusion in the digital medium.

(14) There is a growth and enhancement of the Internet of Things where individuals have also become subject to the compromise of their privacy. Nowadays, everyone is surrounded by the internet for information, both academic and personal. There is much dependence on cyber, and space poses a

threat to our personal information because, most of the time, they need our basic information for using particular services.

(15) Increasing cyber warfare is a new mode of war in the advanced era, which again has a potential destruction method of destroying personal information and other information in the digital medium.

(16) There is a severe threat of a new type of fraud committed with the help of the internet. Everyone is using UPI, Debit Card Payment, and Credit Card Payment for their convenience. Now, the pocket wallet is replaced by E-Wallet. In cases where personal information is compromised, like passwords, that will cause bigger financial loss to the person, and that is also not easily traceable.

(17) Online banking is very common because no one wishes to visit branches of banks, so in the case of online banking, if there is any hacking or intrusion of personal information, that will again cause monetary loss.

SCOPE OF THE RESEARCH

The conceptual analysis and development of data protection-related laws in India are the only aspects of the research issue that the scope of this research will cover. The need for the relevance of data protection law regulation in Indian society and how data is being improperly utilized in several different contexts. The scope of the study focuses not only on the protection of sensitive data but also on the safety of the individual, with particular attention paid to the measures that should be taken before engaging the individual in a variety of cyber activities.

OBJECTIVE OF STUDY

At the beginning of all of the changes mentioned above, India has to enact data protection legislation to ensure the safety of personal information. In light of this, the goals and objectives of the research are based on the issues presented thus far. The following is a list of the goals and objectives that the study hopes to accomplish:

1. To analyse and contrast the data protection laws of the European Union, the United States, the United Kingdom, Canada, Japan, and China, as well as to investigate how the data protection regulations of these countries would interact with data protection law of India.
2. To satisfy the Indian need for a Data Protection Act that adheres to global standards, it is necessary to conduct a study on the standards that are to be

used in the establishment of the laws of these nations and to investigate further the vision of who will gain the most from these laws.

3. To analyze and investigate the current legal landscape of India concerning data protection in other pertinent legislation and the efficacy of these laws over data protection**.**

HYPOTHESIS

1. The extent of the right to privacy is very limited; however, in the era of the internet, it should be enhanced.
2. The present legal system is not appropriate to protect the right to data privacy in the present scenario.
3. Stringent data protection law is urgently required, without which the right to privacy cannot be protected.

RESEARCH METHODOLOGY

The researcher uses a research technique that is a doctrinal, descriptive and non-empirical method to provide appropriate justification for the topic of the study, which allows for a fruitful research conclusion. This research has been done by collecting the determination withdrawn from various books, statutes, reports, and relevant articles. The researcher also utilizes primary as well as secondary sources available for conducting the study of the topic.

In addition, to get further information, the researcher would go through the numerous leading case laws to overview how different branches of the judicial system have interpreted this legislation in light of the issues faced in the modern world.

SIGNIFICANCE OF THE STUDY

The significance of the study is to understand the impact of the advanced era on the privacy of individuals. One is able to protect his personal information data, which is a big question which needs to be dealt with very cautiously. It also provides a platform where one can assume how one’s data is compromised by different entities, whether government or private, without having information to the victim of that unlawful act. This is just the beginning of the understanding of all these activities, which may lead to breaches of privacy and data protection.

LIMITATION OF THE STUDY

This study is limited to different bills presented in the parliament since 2018. The Digital Personal Data Protection Act, 2023, has passed by both houses of

Parliament and also received the assent of The President of India. But this Act has not been notified yet. The researcher faces repetition of literature on the topic. There is also a lack of original text of other countries in the research area. Available materials are scattered in different forms.

SCOPE FOR FUTURE RESEARCH

The scope of this study is limited to data protection, as well as the study of legal rules and policies for data protection and privacy and an examination of national and international laws. There are a significant number of international laws and regulations on data protection in various countries. On the other hand, data protection law of India could be more concrete and may use some improvement. In this study, the researchers conducted an in-depth analysis of all of the national and international statutes that are directly or indirectly connected to data protection and privacy.

This research was carried out using readily available materials, in addition to some bills that were submitted to Parliament. Following the passage of an all-encompassing act, there is a window of opportunity to evaluate the effectiveness of that Act in addressing all concerns of right to privacy as they relate to the field of data protection. Following the passage of the Act for Data Protection, there is also a necessity for an empirical study to be conducted. The findings of that empirical study will allow for some clear conclusions to be drawn regarding the research.

PLAN OF THE STUDY

The whole thesis has been divided into seven chapters. They are as follows:

Chapter-I Introduction

In the first chapter of the study, the researcher tries to introduce the topic of research and methods of the study and also gives the limitations and scope of the study. It includes a basic idea of the research topic and about the right to privacy and data protection. It explains the importance of privacy and data protection in the modern techno-advanced era.

Chapter-II Meaning Concept and Development of Privacy and Data Protection

This chapter explains basic concept of privacy and data protection and how the privacy rights developed towards the protection of data in the modern advance technological era. The earlier concept of privacy begins with protection of information in physical medium but with the advancement of internet the protection is required at higher level**.**

Chapter-III International Legal Framework to Data Protection and Right to Privacy

All the major international regulations are contained in this chapter. The international rules and regulations regarding privacy have started from UDHR, ICCPR, Conventions on the rights of the child, and the Charter on fundamental rights of the EU. It also includes Data Protection Principles and a detailed analysis of General Data Protection Regulation, which is also known as GDPR, 2018. It is a recent development at this level. Most of the European Union countries have prepared their data protection laws as per the established mandate in the General Data Protection Regulation. This chapter also discussed the position regarding the laws, rules and regulations of privacy and data protection in China, Japan, Australia, Canada, the UK and the USA. After analyzing all international instruments, the researcher finds that most of the countries follow the pattern of the General Data Protection Regulation 2016. The countries either legislate the Act according to the norms of General Data Protection Regulation 2016 or they amend their existing laws as per the requirement of that regulation.

Chapter-IV Data Protection Law in India and Right to Privacy: National Prospective

There are so many legislative provisions which have been included in different statutes, regulations, directions, and circulars which operate regulation of privacy and data protection in different sectors of the nation. They are dealing in major segments like Insurance, Banking, and Telecommunication and also in the medical profession. These are so important because it is directly related to the individual information circulating in different regime for availing the necessary services in day-to-day life in commercial activities. In India, though there are many legislative provisions available at the onset of the digital era, there is a need for comprehensive legislation which is able to deal not only with protection in India but also outside India that is cross border flow of personal data.

Chapter-V Governmental Efforts for Data Protection Laws

This chapter included analysis of Personal Data Protection Bill, 2018, Personal Data Protection Bill, 2019 and Digital Personal Data Protection Bill, 2022. In the other part of this chapter, a comparative analysis of the Personal Data Protection Bill 2019 and the Digital Personal Data Protection Bill, 2022 has been done. It also has some other sector-specific draft bills which are under consideration but could not

become law due to various reasons. The government has presented many drafts to defend that they are moving towards protecting the right to privacy and data protection of citizen.

Chapter-VI Comparative Analysis of Protection of Data under Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023

This chapter is divided into two parts. The first part of the chapter discusses the provisions of the Information Technology Act, 2000 and the second part discusses the Digital Personal Data Protection Act, 2023. After the passing of the Act in 2023, there were some amendments to the Information Technology Act of 2000 which included the omission of some provisions. Although the Digital Personal Data Protection Act, 2023 has not came into effect. After coming into effect all the privacy protection of data shall be done by this Act.

This chapter contains an analysis of all the important provisions of the Information Technology Act 2000 related to the protection of data. It also includes an analysis of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. This rule gives an idea about the explanation of sensitive data or information, the collection of that data and the disclosure of data in certain situations. In the second part of the chapter, Digital Personal Data Protection Act, 2023 has been elaborately discussed to understand how data is protected in present digital world.

Chapter- VII Judicial Responses in Protection to Right to Privacy and Data Protection

This chapter contains important cases from the United Kingdom, the United States of America and Canada relating to privacy and data protection. It has also discussed the trends of the judicial system in response to privacy and data protection in India. *K. S. Puttaswamy* v. *Union of India*[1]case is a milestone for changing the perspective of privacy and also accepted as a fundamental right. This chapter provides important facets of national judicial responses and other important judgment from other countries in responses to privacy and data protection. The judgment of Puttasawamy obligates on the Government to legislate a new Act in compliance with that order. But the government has prepared three bills and in but could not pass it till

[1](2017) 10 SCC 1.

the date. There is an urgently need to focus on passing the Act as per the direction of the Supreme Court of India.

Chapter – VIII Conclusion and Suggestion

In this chapter, the researcher suggests certain relevant measures which ought to be taken by the government to protect privacy and data protection in recent times of advanced technology. The researcher also explains certain precautions which are to be followed while working surrounded by digital mediums.

SUGGESTIONS

After doing elaborate and intensive work on the topic, the researcher tries to suggest the betterment of the data protection regime in India. All the suggestions have been discussed as follows-

- Effective data protection also needs to understand the various nuances of privacy risk from digital applications. Apart from risks of direct harms that arise out of illegal surveillance, profiling and possible uncovering of one's private world to the public, the other crucial aspect of privacy is the indirect harms that arise out of invasions that link soiled data items to create digital hallucinations of personae and use them inappropriately. The indirect harms are hard to detect, often because their effects are more subtle and long-term.
- Hence, the measures of post-violation complaints and penalties of the type envisaged in the Digital personal data Protection Act, 2023 are not adequate for protection and mitigation. Protection from indirect harm needs to be ex-ante rather than ex-post, and data fiduciaries and data controllers need to have exacting standards for ex-ante privacy protection and purpose limitation.
- The over-dependence on consent stimulates the possibility of unreasonably putting the onus on unsuspecting individuals to correctly recognize all privacy risks entailed in complicated digital applications; consent is often present false choice. Denying consent in pervasive applications may unreasonably limit options, cause hardship to use that application even affect the freedom of expression.
- Effective data protection requires an accountability-based rather than consent-based framework, which puts the onus on data controllers and fiduciaries, irrespective of the level of consent rather than on the individual. This is not to

say that consent is not required but that one cannot hide behind consent for privacy data protection.

- The standard of anonymization, encryption and access control must be there to protect data privacy. These are not only technical or operational issues but play a crucial role in digitalization and data, without which any data protection discourses, will be incomplete. Even if the details are relegated to subordinate regulation, the objective and standard need to be specified in an effective way.
- Their need to review regular data protection procedures, conduct audits and assessments. This may be helpful in placing necessary safeguard to protect personal data, ensure compliance with regulatory requirement, and identifies vulnerabilities.
- The companies must use strong data security measures, such as encryption, access control, secure coding procedures and routine security testing. Protecting sensitive information requires the use of multi-factor authentication as well as secure data transmission and storage.
- Conducting privacy impact assessment analyses for new initiatives, technologies, and modifications to data-protecting procedures can assist in identifying and reducing privacy risk. The potential effect on privacy of the people should be assessed and the right course of action should be determined to address any risks that are found.
- In modern times the business cannot move smoothly without cross–border transfer of data, which is a crucial part of any business activity. The secure data flows are made possible by international cooperation and the harmonization of data protection law, which also ensures uniform privacy standards across jurisdictions.
- Addressing data breaches involving cross-border data flows necessitates international cooperation. In order to ensure that the rights of those who are impacted are protected, cooperating among data protection authorities enables prompts and coordinated response, investigation and enforcement actions.
- There needs to be development of global standards and best practices for data protection in the industry made possible by international cooperation. Collaborations between regulators, business stakeholders and international organizations promote knowledge, experience and expertise sharing, which result in the creation of strong and efficient data protection frameworks.

- Policymakers, regulators and industry participants should actively participate in international dialogue, share experiences and best practices and work towards harmonizing data protection laws and standards in order to achieve effective data protection in every sector. International collaboration and cooperation will create a more stable, secure and reliable data protection regime.
- There should be proper procedures for collecting the data of individuals, and also specify the purpose of such collection must be provided before collecting such data. There is a mandatory option of informed choice, which is helpful in avoiding future mishandling of data of individual.
- The collected data must be stored in the same jurisdiction, and that data cannot flow outside for processing unless there is a strict regime of data protection law existing at reciprocal system. The storage of data must be secured and in encrypted form by which no unauthorized access to the data is possible.
- Identifying and segregating data on the basis of nature is a precursor for securing the data. The sensitive data must need a higher level of protection as compared to other types of data. The breach of sensitive data may cause greater harm as compared to other forms of data.
- The ownership of data must be clearly defined because when data is collected after informed choice, then in future processing of such data and any gain from such activity lies with the ownership of such data. The actual owner whose data is collected and processed may be at the lower side in getting the benefit of such processing of his personal data.
- Using artificial intelligence in detecting a breach of data protection is one of the best ways to identify the issues at the earliest and also to indemnify that breach within the shortest possible time. The application of artificial intelligence supports the investigation of that breach by technical lapse, and identifying the person who committed such an act is the utmost priority of everyone.
- The application of the principle of non-discrimination in the processing of personal data protects the discrimination on the basis of race, ethnicity, color, sex life, political opinions, religion, philosophical and other beliefs. It means any discrimination data must not be compiled and stored.
- There should be independent supervision and legal sanction, which ensures fair process and accountability at ground level. There should be an authority accountable in law for giving effect to the requirement of data protection. This

fair process and accountability will protect the breach in the ordinary course of processing.

- There should be compatibility in cases of trans border flow of personal data. It is intended to avoid the creation of unjustified obstacles and restrictions to the free flow of data as long as the circulation is consistent with the standard or deemed adequate for that purpose.
- It is strongly recommended that where some decisions impact data subjects legally or significantly, such decisions shall not be taken via automated processing solely. In such instances, there must be a process involving the manual review, which ensures less impact.
- Where there are secondary purposes apart from the primary ones, then there should be a listing of all such purposes and also have protocols in place that will ensure data privacy compliance in instances where secondary purposes come up in that they are different from the primary and other purposes defined.
- When it comes to the secure destruction of personal data, whether in paper or electronic format, there must be processes that set forth acceptable mechanisms for destroying personal data without compromising the security and privacy of such data.
- There must be a definite procedure relating to the use of cookies and similar tracking mechanisms so that relevant privacy risks are mitigated. Organizations must have privacy notices on their websites, etc., that document the use of cookies and similar tracking mechanisms.
- Organization must focus on their personal data retention practices and consider the following elements: limitation or restriction on retention of personal data, requirement relating to litigation hold, compliance, etc., access definition and control and storage of personal data records. There must also be a focus on data or system backup plans.
- In terms of the direct marketing system, organizations must consider certain essentials like the use of valid consent methods, recording customer preferences against do not call, etc., referring to and complying with do not call or do not contact lists where related laws and regulations mention such restrictions.
- In telemarketing practices, organizations must establish standard procedures around aspects such as the kinds of mandatory disclosures to be made during

telephone calls, any usage of auto-dialers, call recording, valid consents, and maintenance of opt-out or do not call lists from those services.

- In digital advertising practices, whether they are mobile or online, organizations must be careful about observing human behavior and then sending targeted ads to people based on their online and mobile behaviors. They must establish control relating to the use of cookies, browser caches, and the use of individual personal information whilst creating profiles and in order to monitor or track user preferences by online or mobile activities.
- To the extent that an organization handles personal data and has employees, vendors, etc., that use social media, it should have social media guidelines made available for employees and vendors. Such guidelines must relate to the active collection of personal data by way of sending friend requests to other employees or customers, etc., and passive collection of personal data by way of individuals posting or commenting on the organization web page, and the use, security and retention of personal data.
- Organizations collect personal data of their employees, visitors, vendors, etc., in order to provide for their safety and security. While this is essential, Organization must ensure that none of these data collection practices go against fundamental data protection and security principles or against the organization's data protection policy. Consideration should be given to personal data collected during accidents or incidents at the workplace and to how this personal data is processed, made, secured, retained, and destroyed after the completion of purposes.
- Most organization implements mechanisms that monitor activity of the employees that may negatively impact the organization or its employees. However, before any such mechanisms are implemented, organizations must check with their privacy guidelines so that privacy issues are addressed appropriately. It is important that one considers the collection of personal data for specific employee monitoring purposes that should be reasonable. There will be instances where valid consent will have to be taken separately. It must be kept in mind that different countries have different laws on employee monitoring, and therefore, a multinational organization must follow the monitoring procedure as permissible in the working country of that organization.

- Any organization that operates CCTVs in its premises must ensure that they have standard procedure on the use of CCTV policy that sets forth the purpose behind having CCTV surveillance, the expected results, the type of technology and equipment used for capturing videos and images, how such videos and images used, stored, kept secure, access control, authorized disclosures etc.
- Where organizations use geo-location devices (like in terms of providing cab services, etc.), they should have a procedure which must be carefully vetted and approved by the concerned authority under the law, which defines the use, purpose, storage, access, control, etc., in relation to the geo-location data, and how and such data is captured, etc. Such a procedure should also include details of consent and notice used, the measures taken to ensure the security of the data, and the option and mechanism for turning off the geo-location tracking capability, if and when required.
- Sometimes, an employee of an organization may be on leave of absence or on holiday or may be terminated. In such situations, there could be a legitimate business need for their supervisor to have access to their email account for a particular period for business continuity reasons. For the facilitation of such situations, organizations must have in place processes in order to authorize access to such employees' email boxes in a way that takes into account privacy concerns. In general, organizations must dissuade employees from using organizational email accounts for personal reasons.
- If any organization engage in any high-risk project or processing activities must conduct data privacy impact assessment at regular intervals. Whether any process is at high risk can be understood by some examples like the application of artificial intelligence, smart technology (including wearable), credit checks, social media networks, workplace access systems or identity verification, DNA testing, etc., where data privacy impact assessment is required, organization must seek advice from a concern authority or privacy professional.
- There should be the option of data portability available to every individual. It provides a fair and competitive environment for the processing of individual data. In case any individual is not satisfied with the processing, he has the option to change the service provider for processing of her data. This definitely gives more transparency in the process of data of an individual for a specified purpose.

- There should be an independent body present in the country for entertaining the data breach incident of an individual. This concept has already been working in some countries like Canada has an independent civil society type body which can investigate independently the data breach incident.
- Whenever choosing any online service where age criteria are fixed in that situation, age verification for availing of those services must done properly with certain established guidelines. Without that verification, that service must not be activated.
- The public and private sectors should collaborate on educational programs to raise awareness about data protection and privacy rights among the Indian population. Ethical principles should be integrated into data protection, addressing algorithmic bias and discriminatory data practices.

****