INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 4 | Issue 1 [2026] | Page 33 – 51

NAVIGATING PRIVACY LEGISLATION IN INDIA WITH SPECIAL EMPHASIS ON DIGITAL PERSONAL DATA PROTECTION ACT

-Girish Anupama Turup[1]

ABSTRACT

For many years in India, people have been trying to figure out if the Right to Privacy is even important. Does the Right to Privacy fall under the fundamental rights, The constitution had no where expressly mentioned that the right to Privacy is a fundamental right. Hence the Judiciary interpreted the Right to Privacy in various cases. Firstly it held that the Right to Privacy is not a fundamental right but later in the case of Puttaswamy Vs Union of India, it held that the Right to Privacy is a part of the Right To Life guaranteed under Article 21 of the constitution.

India never had an exclusive law regarding data privacy. Information Technology Act 2000 had a few Sections that dealt with data privacy. The rules of 2011 was also introduced to protect sensitive information. Finally, after many drafts were made and passed the Digital Protection and Data Privacy Act was implemented in 2023.

The present project deals with these question and also in detail about Right to Privacy, the Sections under Information Technology Act, The IT rules 2011. The project also deals with the understanding of the new act Digital Personal and Data Privacy which is the first legislation in India that talks solely regarding data privacy. It also includes the impact of the new law on various business like the E-Commerce platforms and the SaaS (Software as a Service).

INTRODUCTION

Privacy as a term is not defined in any act or law but it can be defined as a human right that should be available to every human being. It can also be defined as a Right to keep personal information private.

[1] Registered with Telangana State Bar.

The word private is derived from the Latin word *'privatus'* which means something that is personal or secret. The word opposite to public which includes all the people is the word private which means something that provides for the individual.

Privacy was a term used to define the right to be let alone and ought to be let alone. The right to be let alone is something that an individual has since the time of his birth but ought to be let alone is something that the legislation or the laws provide to the individuals. In other words it can simply be defined as a right to enjoy his owns presence by himself. Privacy as a right is very essential for the protection of the dignity of the individual.

Privacy is essential for personal autonomy which is necessary for individual development and growth. It is necessary for the emotional release of an individual. In the present times any individual faces immense pressure and tension which requires privacy to relax and ease down. Privacy is also important for self evaluation and decision making. It is necessary that any individual is given his space to make decisions for himself.

There are not much legislation that talks about privacy or data regulations. However there were amendments made to Information Technology Act 2000[2] that had few Sections that dealt with the term privacy and data protection. The rules were also introduced in this aspect but there was never proper legislation for this until 2023 when the Digital Personal Data Protection Act[3] was implemented. This was a proper Act or legislation just for privacy and data protection.

Privacy has a both positive and negative impact on individual. As we understand that privacy is essential for the dignity of the individual it is also necessary that it must be reasonable in nature. Privacy as a term can be completely misinterpreted and have negative impact on society. It is necessary that the government has information of every individual in the country for various purposes. Hence in such case the individual cannot curtail himself from presenting such information on the name of privacy.

HISTORY

This term privacy was first witnessed in the case of Semayne which dealt with the right of privacy in the year 1765. Since then many countries made different laws to protect the privacy of their citizens.

[2] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[3] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

The GDPR formed in 2016 was one of the most important regulation made for the protection of individuals privacy. The major importance of this regulation was that it gave the right to the individuals to request the information holder to delete their personal information. This GDPR became a source of many laws in different nations. The Indian new law of Digital Personal Data Protection Act 2023 was also inspired from the GDPR.

In India, the first case that dealt with the concept of privacy was Nuth Mull Vs Zuka Oollah Beg and another in the year 1855. This case explained that it is necessary that before entering any person's house or property it is necessary to take the permission of the individual who owns or resides there. The framers of the Constitution also tried their best to include the term privacy as an individual right. Privacy in India was never discussed as a part of any law. There were numerous debates regarding the word in the Parliament while drafting the Constitution; hence, it was finally decided that it would not be added in the Constitution as a part of the fundamental rights. The Judiciary however dealt with the term privacy in many cases. The Judges had given various interpretations on why they would not consider the term as a part of the fundamental rights in the initial cases.

RIGHT TO PRIVACY A FUNDAMENTAL RIGHT?

The right to Privacy is not expressly mentioned in the Constitution. The Courts in various cases interpreted whether the Right to Privacy is a part of any existing Fundamental Right.

The case of MP Sharma Vs Satish Chandra[4] and Kharak Singh Vs State of UP[5] even though did not directly mention the word Privacy dealt with it. In both these cases, the Courts did not accept that the Right to privacy is part of the fundamental rights guaranteed under the Part III of the constitution. In the Kharak Singh case the Judges were of the opinion that night visits tot the house of the appellant were against his fundament right to life and liberty. The minority opinion of Justice Subba Rao held that any surveillance activity conducted is violative of the fundamental right of life and liberty and hence unconstitutional.

The first case in India that openly discussed the term privacy was Govind Vs State of Madhya Pradesh[6] in which even though it did not consider the Right to Privacy as a fundamental right it held

[4] MP Sharma Vs Satish Chandra 1954 AIR 300

[5] Kharak Singh Vs State of UP 1963 AIR 1295

[6]Govind Vs State of Madhya Pradesh 1975 AIR 1378

that this right emanates from the right to move freely, right to speech and right to liberty but it should not be an absolute right with respect to the public interest.

The Courts by this time were considering the Right to Privacy as a part of the Right to Life and Liberty guaranteed under article 21 of the constitution. Though it was not expressly said that the right to privacy was a fundamental right they considered this right as an important right of every individual. In the case of Rajagopal Vs State of Tamil Nadu[7] famously known as the Auto Shanker case where the Court held that the publication of the person's life story without his consent was against his Right to privacy and entitled him to compensation as it was an unauthorized invasion of his privacy. In the case of PUCL Vs Union of India[8] where the court struck down Section 5 of the Telegraph Act where the CBI had power to intercept the phone conversation without fair and reasonable safeguards as unconstitutional as it violated the Right to privacy of that person. These were some cases where the Judiciary interpreted the Right to privacy.

In this case of Mr X vs Hospital Z[9], the matter was regarding the disclosure of the appellant's health issues by the doctor to any family member. The appellant held that this was a violation of his right to privacy. On the other hand the doctor had revealed it to his fiance who would have suffered if she was not aware that he was suffering from HIV which was a sexually transmitting disease. There was a clash between the right to be left alone and the right to be informed and in this case if she wouldn't know would effect her fundamental right to lead a healthy life guarented under Right to life. The judges had finally decided that it was necessary to inform the fiance that the guy she was about to marry was suffering from a sexually transmitting disease and hence decided it against the appellant

In this case of Sharada vs Dharmpal[10] the court dealt with the question whether the right to privacy is absolute or not. The case here was that in case a party seeks divorce on the basis of impotence then the court can order for medical examination. The Court cannot conclude without a medical examination and hence in such cases it can order for medical examination. This the right to privacy cannot be held absolute but it is important that the consent of such individual is obtained before such examination.

---

[7]Rajagopal Vs State of Tamil Nadu 1995 AIR 264

[8]PUCL Vs Union of India AIR 1997 SC 568

[9] Mr X vs Hospital Z AIR 1999 SC 495

[10] Sharada vs Dharmpal AIR 2003 SC 3450

This case of BHABANI PRASAD JENA VS. CONVENOR SECRETARY, ORISSA STATE COMMISSION FOR WOMEN & ORS[11] is also similar to the previous case where the issue was relating to the DNA test for examining the parent of the child. The judges were of the opinion that unless it is very important and with the consent of the individual while examining the effect of such examination on the child should the Court order a DNA test.

In this case of GIRISH RAMCHANDRA DESHPANDE VS. CENTRAL INFORMATION COMMISSIONER & ORS[12] the Court held that personal information of any public officer would not be revealed under the RTI Act as it amounts to privacy of the individual. The Court held that service related matters is something between the employee and the employer and no other individual has the right to question it.

The case of Justice K.S.Puttaswamy(Retd) Vs Union of India[13] was a landmark case for the Right to Privacy where a nine judge bench overruled the judgments of MP. Sharma and Kharak Singh where the eight and six bench respectively had ruled that Privacy was not part of the fundamental rights guareenteed under Part III of the constitution.

The UPA government in 2009 launched the AADHAR to collect every individual's data to prepare a centralized database. In 2010 Unique Identification Authority of India started enrolling the Indian citizens in this Aadhar scheme. This contained the individual's name, age, gender, address, phone number and other confidential information such as fingerprints, iris scanning were recorded. Many felt that this Aadhar was breaching the privacy of the individuals and in a democratic nation, the government should not have such confidential information of the citizens. One such person criticizing was the High Court rtd Judge K.Puttaswamy who in 2012 filled a writ under Article 32 of the constitution before the Supreme Court as Aadhar was violative of the Right to Privacy and hence is unconstitutional. He also pleaded that the Right to privacy is a fundamental right and hence it needs to be protected. While the writ petition was still pending the Parliament passed the Aadhar Act. The petitioners moved another writ to challenge the constitutionality of this Act.

[11] BHABANI PRASAD JENA VS. CONVENOR SECRETARY, ORISSA STATE COMMISSION FOR WOMEN & ORS AIR 2010 SC 2851

[12] GIRISH RAMCHANDRA DESHPANDE VS. CENTRAL INFORMATION COMMISSIONER & ORS 2012 AIR SCW 5865

[13] Justice K.S.Puttaswamy(Retd) Vs Union of India AIR 2018 SC (SUPP) 1841

The issue in this case was whether Aadhar violated the fundamental rights of the citizens. The next was whether Right to privacy was a fundamental right while the third was whether a few provisions of the Aadhar Act like linking mobile numbers and bank accounts be struck down.

The judgment declared by Supreme Court was that it overruled the decision of the MP. Sharma and Kharak Singh and declared Right to Privacy as a fundamental right under Article 21 of the Constitution. It held that privacy excluded the interference of state in the individual's personal space like family, marriage, sexual orientation and procreation as a integral part of dignity which must be protected.

EFFECTS OF PUTTASWAMY JUDGMENT

This was a very landmark judgment in India as this declared that Right to Privacy is also a part of the Fundamental rights which later became a precedent to many judgments.

With this decision being the precedent the Supreme Court in the case of Navtej Singh Johar Vs Union of India[14] held Section 377 of the Indian Penal Code as unconstitutional. This section considered any unnatural sex as an offence which made any homosexual couple an offender. The Puttaswamy case considered that sexual orientation was also part of the privacy of the individual and hence considering them as offenders merely because of their sexual orientation was not correct.

In the case of Salamat Ansari And Others vs State Of U.P. And Others[15] also Puttaswamy case was used as a precedent where the inter-caste marriages were held valid. It was held that privacy is a part of an individual's dignity and hence it must be the right of the individual to make his choices regarding marriage, children, etc. The Allahabad High Court in this case upheld the validity of the right of choice in inter-caste or inter-religious marriages.

In the case of Faheema Shirin. R.K vs State Of Kerala[16] the issue before the Kerala High Court was regarding the right to the Internet. In this case, the hostel students that is the petitioners were suspended from the college for using mobiles against the rules framed by the college. The Court held that rules should be made in such a way that it should blend with the current scenario and students require mobiles and laptops for education in the present times. It held that in the Puttaswamy

[14] Navtej Singh Johar Vs Union of India AIR 2018 SC 4321

[15] Salamat Ansari And Others vs State Of U.P. And Others AIRONLINE 2020 ALL 2380

[16] AIR 2020 KERALA 35

judgment the Court held right to Privacy as a integral part of liberty of individual. Taking this judgment as precedent the Court in this case ordered the College to re-admit the students.

In the case of Joseph Shine Vs Union of India[17] which challenged Section 497 of Indian Penal Code which talks about Adultery. The Supreme Court taking the case of Puttaswamy Vs Union Of India and held that sexual autonomy and sexual the privacy of the matrimonial sphere must be protected. It gave the parties the option to do wath they decide either divorce or otherwise and initiation criminal proceedings against them would serve no purpose.

RIGHT TO BE FORGOTTEN

The Right to be Forgotten is connected to the Right to Privacy. Right to privacy means the exclusion of the personal information of the individual from being published while the Right to be Forgotten means the exclusion or removal of the personal information from public resources. In the present times, everything is available online and every action of an individual has a trace on the internet. Hence it becomes necessary that the right to be forgotten be included as a right to the individuals. For example, the accused has the right to be forgotten in case where he has not been convicted.

In the case of *Google v. Agencia Española de Protección de Datos, Costeja Gonzalez*[18] *(2014)* were the European Court recognised the Right to be Forgotten. It ruled that citizens can get their names removed from the search engine in case it is no more relevant. It further stated that this right cannot be granted particularly where the publication was practicing their Right to freedom of Speech.

In the case of Rout v. State of Odisha (2020) the Court in India identified the right to be forgotten as a part of the Right to Privacy. It held that it is the right of the victim to get materials removed from online platforms if it is against the dignity of such individual.

In the case of, Jorawer Singh Mundy v. Union of India[19] the Court had ordered for not providing access to the people online regarding the case where it was acquitted of NDPS Act. In this case the petitioner was an Americian citizen who was charged under the NDPS(Narcotics and Psychotropic Substances Act, 1985) but was later acquitted for the same.

He was not able to get a job in America because of his name in the IndianKanoon and other websites. He filed a petition for the removal of his judgment from the online sites. The Courts granted him an

[17] AIR 2018 SC 4898

[18] C-131/12, ECLI:EU:C:2014:317

[19] 2021 SCC Online Del 2306

interim relief and ordered for the removal of his judgment from the online platforms and also blocked any results arising from the search of his name.

DATA PRIVACY AND DATA PROTECTION

Data of an individual now a days is being collected everywhere. Any tourist place we visit or any restaurant or an website that we open ask for the individual's personal information. It majorly demands for Name, Address, mobile number, e-mail address, etc.

The terms data privacy means to handle the personal information or data of an individual and it maintains secrecy and control the access of data by any other person or a third party. For example in any bank many people have their accounts through which they transact their money, hence it is necessary to protect the personal data of the individual customer. The financial records, medical records, names, date of birth, contact numbers, ID proofs, Address are certain information that needs to the protected. Data privacy ensures that the personal information shared to an single entity or organization remains with only the authorized parties. Data privacy is regulating the information or data through policies.

Data Protection on the other hand is keeping the sensitive information or personal data safe from any unauthorized access. Data Protection is necessary for not only personal data but also organizational data or any general data as well. It is necessary that any organization or institution that collects data also has the obligation of handling and protecting the data from any corruption, loss or harm. Data Protection can be done through proper implementation of procedures and mechanisms to protect the information.

There are many technologies that can be considered as a hindrance or against the right of privacy but for the current generation these technologies are very important. One of them being cctv cameras that not only is used by the government to monitor the individuals but also private persons use them for their individual protection. Second thing is bio metric identification which is necessary information that the government has for providing benefits for the people. It includes the fingerprints, iris, voice patters etc which can be considered curtailing the right of privacy if they are obtained without the consent of the individual.

Internet now a days is also a platform that has immense data. Any information can be gathered from the internet. Data chips or cards are also other technologies that effect the privacy of the individual.

Maintenance of various ID cards or licences in a digital form through various cards or apps can also effect the privacy hence it must be carefully protected.

IT ACT 2000

Information Technology Act 2000[20] was introduced with the intention to enforce sanctions to computer misuse and also to provide legal recognition to the e-commerce platform. There were no provisions that dealt expressively with data protection. However the Section 43 talked about Penalty and compensation for damages to computer or computer systems which included the damage of any data from such device and Section 66 talks about Computer related offences and mentions elaborated on Punishment for offenses mentioned under Section 43 of the IT Act.

Information Technology Act 2000 was the first legislation to include the aspect of Data Protection. Section 43 A of the Act explains that if any body corporate processes, handles or deals with any sensitive personal data in a computer resource that it owns, controls, or operates is negligent in maintaining or implementing reasonable security practices and procedures and such negligence causes wrongful loss or wrongful gain to any other person then such body corporate shall be liable to pay damages by the way of compensation to the person affected.

The word body corporate according to this section means any company, firm, or other association of individuals associated with commercial or professional activities.

The word reasonable security practices and procedures means practices and procedures designated to protect such personal information from unauthorized access, damage, use, disclose or modification as specified by the agreements between the parties or specified under any law in force and in the absence of both then as prescribed by the Central Government in consultation with professional body or association.

The word sensitive personal data or information means such personal information as may be prescribed by the central government in consultation with professional bodies or associations as it may deem fit.

Section 72 of the Information Technology Act talks about penalty for breach of confidentiality and privacy. It explains that if any person who has the power under this act, rules or regulations has secured access to any electronic record, book, register, correspondence, information, document or other

[20] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

material without the consent of such person discloses the information to any other person will be punished with imprisonment of term not exceeding a term of two years or fine that can extend upto one lakh or both.

Section 72A talks about the punishment for disclosure of information in breach of a lawful contract.

INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011[21]

Defining 'Sensitive Personal Information'

Section 3 of the Information Technology Reasonable security and procedures practices and sensitive or Information) Rules, 2011 apply only to body cooperates and individuals acting on behalf of the body corporate. These rules define the term personal information as any information of a natural person that either directly or indirectly or in combination with already available information may identify the person. It includes information such as:

(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:

provided that, 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 shall not be regarded as sensitive personal data or information for the purposes of these rules.

[21] https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

These rules regulate Collecting, receiving, possessing, storing, dealing, handling, retaining, using, transferring, and disclosing sensitive personal data or information, Security practices and procedures for handling SPDI, and Data subjects' rights to review and update SPDI and withdraw consent for SPDI processing.

Based on the definition of personal as defined in the regulations, it can be inferred that these regulations intend to protect personal data that makes a person identifiable. Some of the regulations go a step further in defining the sensitivity of this personal data. sensitivity personal data includes information about individuals political opinions, religious belief's, sexual preferences, etc. and its definitions may vary with the country/region where it is defined as each country/region has its own data privacy culture. For example, caste of an individual may be considered sensitive in some countries through it may not constitute sensitive in their respective cultures and should define sensitive personal information accordingly.

The rules are provide for certain rights for the person who provides such personal information to the body corporate. The information cannot be collected by the body corporate without the prior consent of the person who the information belongs to. The person also has the power to withdraw the consent given to collect such sensitive personal information.

The rule 6 of the 2011 rules specifies about that the body corporate has to take necessary consent before sharing or publishing the data to any third party. The exception to this rule is either that the information was used for compliance of any legal obligation or if the information provider and the body corporate already had agreed for it in the contract. The provider of the information has the power that any time he can review and amend it if he finds any information to be inaccurate.

These rules also specify that the body corporate has to utilise the information only for the purpose it was taken and not for any other purpose. It is also necessary that the body corporate has to hold the information for no longer time than to satisfy the lawful purposes for which it had been collected.

In case there is any grievance to the information provider it must be resolved by the grievance officer of the body corporate within one month of such complaint. It is necessary for the body corporate to provide the information of the grievance officer on the website.

The rules explain that the sensitive personal data or information can be transferred to any other body corporate or a person in or outside India but it is necessary that they also maintain the same level of data protection. This must be according to the contract between the information provider and the body corporate with prior consent of such transfer.

DATA PROTECTION BILLS

The need for privacy legislation was important after the landmark decision of the Puttaswamy Vs Union of India where the Supreme Court had recognized the Right to Privacy as a part of the Fundamental Rights under Article 21 of the Constitution. There were several drafts made for the Privacy legislation. The first draft was named as the Draft Personal Data Protection Bill (2018). This was framed immediately after the Supreme Court's landmark judgment.

The second draft was the Personal Data Protection Bill (2019) while the third was named the Data Protection Bill (2021). The Bill of 2021 which was supposed to be helpful to the user with the right environment did not prioritise the user. It in stead provided large exceptions to the Government Departments and big corporation while ignoring the fundamental right to privacy.

The Minister of Communications and Information Technology had withdrew the bill of 2021 with reason that it wanted to accommodate the suggestion made by the Joint Parliamentary Commission on the PDPB 2019 to make comprehensive legislation to address the technology issues in the country.

DIGITAL PERSONAL DATA PROTECTION ACT 2023

The Digital Personal Data Protection Act[22] was passed by Parliament in August making it the first Act relating to the protection of an individual's personal data. This act focused on having a balance between maintaining the privacy of an individual's data and the need to process such data for lawful purposes. The drafts or the bills were introduced after the Puttuswamy and another Vs Union of India 2017, where the Court held that the Right to Privacy was part of the Right to life guaranteed under Article 21 of the constitution. This act includes provisions regarding consent, legitimate use, breaches and data fiduciary, processor responsibility, and individual's right over data. The Act does not apply to information to data processed for law enforcement or national security purposes.

22 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

DEFINITIONS

PERSONAL DATA

Data is defined under the act as a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings.
The act defined personal data as any data about an individual who is identified by or in relation to such data.
The data can be Name, Address, Date of birth, Gender or other information that reveals the identity of such person or other information relating to him is personal data.

DATA FIDUCIARY

Data fiduciary as defined under the act means any person who alone or in conjunction with other persons determines the purpose and means of processing personal data.

DATA PROCESSORS

The act defines Data Processors as the people who process personal data on behalf of the data fiduciary.

KEY PRINCIPLES

1. Lawfulness- The possession of data must be done in a fair, lawful and transparent manner.
2. Purpose Limitation: Personal data must be collected for specified, explicit, and legitimate purposes and not in a manner that is incompatible with those purposes.
3. Data Minimization: Personal data must be adequate, relevant, and limited to what is necessary to be processed and not in furtherance.
4. Accuracy: Personal data must be accurate and, where necessary, kept up to date.
5. Storage Limitation: Personal data must be kept in a form that permits identification of data subjects not more than the time it is required to be kept.
6. Integrity and Confidentiality: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organizational measures.

OBJECTIVES OF THE ACT

The major objective of this act is to protect the data of an individual. This act defines the term data fiduciary and imposes certain obligations concerning handling and protecting the data of a data principal. This act provides for the rights and duties of the data principles. It also provides for a proper redressal mechanism firstly by the data fiduciary and then from the Data Protection Board of India established for the very purpose of dealing with the data breach or other privacy-related matters under this act.

SALIENT FEATURES

1. This Act applies to non-citizens living in India as well whose data processing is done relating to any activity of offering of goods and service.
2. The Data can be processed on the grounds of legitimate use and when the data principal has given consent. The consent must be fair, specific, and unconditional with clear affirmative actions.
3. Along with consent, the data fiduciary must also send a notice regarding the purpose of the information, her rights, and the manner of filing a complaint.
4. The rights of individuals include
    a) the right to get a summary regarding the data collected,
    b) the information regarding the data fiduciary, and the data processors with whom such information will be shared.
    c) the right to correction, completion, updating, and erasure of the data.
    d) the right to redress their grievances and
    e) the right to nominate.
5. There are certain duties of data principals include
    a) to comply with the provisions of the Act,
    b) to be truthful while providing the information
    c) to not to impersonate someone while sharing the data
    d) to not to register a false complaint with data fiduciary or the board.
6. The obligations of data fiduciary include:

(a) maintaining security safeguards

(b) ensuring completeness, accuracy, and consistency of personal data

(c) intimation of data breach in a manner prescribed to the Data Protection Board of India (DPB)

(d) consent of an individual for data erasure, withdrawal, or the expiry of the specified purpose

(e) the data fiduciary has to appoint a data protection officer and set up grievance redress mechanisms

(f) the consent of the parent or guardian is mandatory in the case of children or minors.

7. The Government will appoint Significant Data Fiduciaries based on the volume and sensitivity of the data risk to data principle and impact on sovereignty and integrity. The SDF will have additional obligations such as appointing of Data protection officer who is answerable to the Board of SDF and acts as a point of contact with redressal mechanism. SDF also has to evaluate the audits and the Data protection impact assessment.
8. The Government can restrict the flow of data to any particular country for national security purposes.
9. The notice and certain obligations of the Data fiduciary requirements are not compulsory in cases where the processing of data is necessary for enforcing legal rights or claims. The personal data can be processed by courts and tribunals or in case of prevention, detection, and investigation of an offense. It also includes the financial information of the person who has defaulted on the payment. It also includes certain classes of data fiduciaries including startups excepted from the provisions like notice, competence, accuracy, consistency, and erasure.
10. The provisions of the act shall not apply in case the data is processed to maintain sovereignty, integrity, and public order. The other case is if the data is being used for research, archiving or statistical purposes but such data shall not be used to make a decision on the data principle.
11. The act also provides discretionary powers to the government to notify any data fiduciary within five years of the commencement of the act to be exempted from the provisions of the act.
12. The Data Protection Authority of India is established as an independent authority responsible for the implementation of the Act. This Authority has the power to investigate complaints, issuance of fines and compile organizations to follow the act.
13. In case aggrieved by the decision of the Board then within 60 days the matter can be appealed to the Appellate Tribunal.
14. In case of breach of any provision of the Act after giving an opportunity of being heard monetary penalty can be imposed.

DATA PROTECTION BOARD OF INDIA

The Chapter V of the Act talks about the Data Protection Board. The Central Government shall establish the Board and it shall be a body corporate with perpetual succession. The Board shall consist of a Chairperson and other members as the Central government may deem fit. The Chairperson and members shall be people with specialized knowledge in the field of data governance, administration or implementation of laws, information and communication technology, dispute resolution etc. Out of all the members, at least one member should be an expert in the field of law.

The powers of the Chairperson includes:

a) He can give directions to the board relating to any administrative matter and have superintendence.
b) He can appoint any officer to scrutinize any complaint, reference or correspondence addressed by the board.
c) He can conduct any proceedings and also authorize performance of any functions of the Board.

Chapter VI of the Act specifies the powers and functions of the board.

IMPACT ON SERVICE PROVIDERS

SaaS Software as a Service is a cloud computing model that revolutionizes software applications. It provides services, wherein instead of purchasing the software individually a third party hosts and maintains the software. It will be available on the internet and its services can be utilized after the payment of the subscription amount. Since the market for SaaS is growing it becomes necessary to have certain rules for them to handle the data with utmost care, hence they need to adhere to the guidelines mentioned in the Digital Personal and Data Protection Act.

The major impact on these service providers is that the obligations must be followed properly such as:

a) Consent- The consent must be obtained from the users as well as employees and it should be freely given and specific. However, in certain situations, service providers are not required to take the consent where it is for legitimate use.
b) In the case of Children's Personal data the SPSPA requires the consent of the parent or the guardian to be taken. To reduce their liability the service providers are establishing a minimum age for the users.

c) In case of Cross Border Data Transfer where the service providers are based outside India provide services within India are also required to adhere to the DPDPA.

IMPACT ON E-COMMERCE BUSINESS

E-commerce businesses also use data for targeting, analyzing, and marketing their product. Hence they must handle the personal data of the customer with utmost care. The DPDPA imposes certain obligations on the data fiduciary who determines the purpose of processing personal data to limit and protect the data. It also provides for various rights for the data principals. The main aim of the act was to promote better responsibility for the companies handling personal data.

The impact on the consumer business due to the DPDPA is as follows:

a) Expressed Consent must be taken by the businesses before collecting or using the personal data. The consent obtained must be freely given, specific and unambiguous.
b) The businesses must collect the data only limiting to the purpose it was obtained for.
c) Data must be complete, accurate, and updated.
d) Data must be protected by the businesses with the utmost care from unauthorized access, use, or disclosure.
e) In case of any breach they must notify the data principal.
f) In case the data principal is a minor then the consent of the parent or guardian is necessary.

The major issue becomes the identification of the data fiduciary. It is important to determine whether the platform provider is the data fiduciary or the retailer. The retailers also use personal data to execute or process the orders, hence they can also be considered as data fiduciary. In case the retailers are only involved in the business of goods and services and receive no personal information they cannot be called as data fiduciary.

In an E-Commerce business, the platform provider is the main data fiduciary as he collects large amounts of personal information such as Name, Address, Phone Number, E-mail address etc. Hence it becomes his obligation to maintain

DRAWBACK OF THE DPDPA

Even though this legislation was bought solely to protect the data of individuals, it has certain loopholes in it. They include

1. This act does not provide compensation or any other remedy for the Data Principal in case of a data breach.
2. This act does not deal with sensitive data protection.
3. The delegation under this act is excessive and may lead to the exercising of power in a way that is arbitrary by the authorities while making decisions.
4. The Data Protection Board is appointed by the Central Govt thus arising the questions relating to its independence.
5. This act does not contain provisions relating to data portability which was included in the 2019 bill.
6. The exemptions to government is another major drawback as it exempts the government from receiving consent before data processing of the individual for security purposes or maintaining public order.

CONCLUSION

Privacy is a term that needs to be interpreted carefully. On one side it is the most important right that ensures the dignity of an individual and on the other side, there must be reasonable restrictions imposed. These restrictions are necessary so that one individual does not over step into the privacy of another individual. It is also important that certain information of citizens must be known to the government.

Privacy and data protection are very important in the present times. There should be proper rules and regulations to make sure that the privacy of every individual is protected. After long time the Indian Government now recognised the need of a law that solely talks about privacy and data protection.

The new act of Digital Personal and Data Protection Act 2023 is not implemented yet. This act is also not very specific in the sense that it does not talk about sensitive personal data and just talks about data. This act also gives so much power and exceptions to government where it specifies that they do not require to take the consent of any individual before acquiring or transferring personal information of any individual.

Hence the Government has to bring more serious and strict laws for data protection as the current world is completely shifting to virtual mode. Almost every data of an individual is being exposed on various social media platforms. Not only these but various devices like GPS track the location of an individual which is a major threat to any individual. Even though these technologies are important they must not curtail or misuse the data of the individual.

BIBLOGRAPHY

- https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
- https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf
- https://blog.ipleaders.in/relevance-of-sensitive-personal-data-information-rules-2011-in-2021/
- https://www.lexology.com/library/detail.aspx?g=174412a6-fa19-4055-90f9-dec6bb229ac1