THE LAWWAY WITH LAWYERS JOURNAL
VOLUME:-20 ISSUE NO:- 20 , MARCH 25, 2025
ISSN (ONLINE):- 2584-1106
Website: www.the lawway with lawyers.com
Email: thelawwaywithelawyers@gmail.com
Authored By :- Anamika Das

DATA PRIVACY UNDER THE INDIAN LEGAL SYSTEM

ABSTRACT
Data privacy is individuals' right to control their personal information. Information privacy is another name for data privacy. In the modern world data is an asset for every human being. Data is a collection of facts such as numbers words descriptions of things. But nowadays many evil people are misusing people's data. If people do not have control over their data evil people can use it in many ways like they can use personal data to fraud or harass someone they can selling data or they can track a person's activities and many more things. The Digital Personal Data Protection Act 2023 (also known as the DPDP Act or DPDPA 2023) plays an important role in data privacy. It recognizes the right of an individual to their data and the need to process and search personal data for new lawful purposes and matters connected therewith or incidental thereto. The primary aim of this article is to look into various provisions and the legal fame worth in India relating to data privacy. This article also talked about what is data, why there is a need for data privacy, how people can misuse other people's data, and the importance of data privacy. This article also gives a deep understanding of the Digital Personal Data Protection Act 2023.
Keywords:-
Data privacy, right, data protection, personal data, digital, court, act, information, right

INTRODUCTION

Data privacy is a very essential right of people in the digital world. Data is the collection of facts, such as numbers, measurements, observation, and even just description of things. Data privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. Under the digital personal data Protection, Act 2023 only includes those data which is digital. It does not include other forms of data. Every user has the right to know how much a company holds their data. They also have the right to access their data. A company cannot use people's data without their permission. If a person wants, they can ask the company to delete their data and the company needs to do it. If the company refuses to do so, that person can file a suit against that company.

Background

On 24th August 2017, A nine-judge bench headed by Chief Justice J. S. Khehar gave a landmark decision on the right to privacy. In 2018, The Srikrishna Committee submitted the draft Personal Data Protection Bill. The draft bill is introduced in Parliament but lapses due to the dissolution of the Lok Sabha. Again in 2022 the government withdrew the bill and introduced a new draft, the Digital Personal Data Protection Bill. And in 2023 the DPDP Act was passed by Parliament and received presidential assent, becoming a law. The law came into effect on August 11, 2023, after being passed by both houses of Parliament and receiving the President's assent.

What is data?
According to the Digital Personal Data Protection Act 2023 section 2(h) data means a representation of information, facts, concepts, opinions, or Instructions in a manner suitable for communication, interpretation, or processing by Human beings or by automated means. This act balances the rights of individuals to protect their data with the necessity of processing such data for lawful purposes.

Why there is a need for data privacy
Data is the oxygen of the digital world. Everything is surrounded by Data in the digital world. Anyone can take our identity by our data. That's why data privacy is very important. Data privacy safeguards our personal identity, rights, and digital freedom and ensures that sensitive data like Social Security numbers, bank account details, addresses, health information, and locations remain secure. One one will be able to use people's data without their consent Or sell anyone. Data privacy also creates a trustful bond between the individual and the organization. If there is no data privacy, people's emails could be hacked and their identities could be stolen and their medical conditions could be shared without their consent, their banking data could be hacked. This call can cause mental, physical, and financial harm.

Challenges in data privacy
Data principals and data fiduciaries both parties face some challenges in data privacy. According to the Digital Personal Data Protection Act 2023, Data Fiduciary means any person who alone or in conjunction with other Persons determines the purpose and means of processing personal data and Data Principal means the individual to whom the personal data relates and Where such individual is a child, includes the parents or lawful guardian of such a child And a person with disability includes her lawful guardian, acting on her behalf. Cookies often record user's activities. In some websites, there is an alert for cookies and in some websites, there is no alert system for cookies policy. In this way, the Data principal's behavior is often tracked online. In some websites, there is a lack of transparency about the website policy. Even the data fiduciary also faces many problems like they unable to communicate with the users about how much data they are taking, how much data they are going a store, and in which way they are going to use users' data. Some third parties also try to hack data leading to a massive data breach; even some insider employees can use users' data inappropriately. That's why the data principles and data fiduciaries need to be alert about their data.

Data privacy Laws that govern data around the world

California Privacy Rights Act (CPRA): The California Privacy Rights Act (CPRA) was passed in November 2020. Amending the recently passed California Consumer Protection Act (CCPA) 2018. It governs companies and individuals that collect and process consumers' Personal Information.
China's Personal Information Protection Law (PIPL): China's Personal Information Protection Law (PIPL) came into force on November 1, 2021. It restricts data controllers and processors on various matters and safeguards individual rights.
General Data Protection Regulation (GDPR): The GDPR came in 2016 and went into force on May 25, 2018. It protects individuals' fundamental rights, especially their right to privacy and protection of their data. Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden, Iceland, Liechtenstein, and Norway covered under GDPR and The UK has its version of the GDPR that applies in a similar way to the EU GDPR.
The Digital Personal Data Protection Act 2023(DPDP Act or DPDPA): The India Digital Personal Data Protection Act 2023 (DPDPA) came into effect on September

1, 2023, and it applies to all organizations that process the personal data of individuals in India. It safeguards the privacy of individuals in the digital age.
And there are many more laws around the world. Examples- Artificial Intelligence Act, Information Privacy, New Zealand Privacy Act, etc.

Importance of Digital Personal Data Protection Act 2023 (DPDPA) in India

Digital Personal Data Protection Act 2023 (DPDPA) is applicable within the whole of India where data is collected online, or offline and is digitized. It will also apply to such processing outside India if it is for offering goods or services in India. This is An Act to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. This act was passed by Loksabha on 7 August 2023 and passed by Rajyasabha on 9 August 2023. Personal data may be used only for a lawful purpose upon consent of an individual. Consent may not be required for specified legitimate uses such as the voluntary sharing of data by the individual or processing by the State for permits, licenses, benefits, and services. This act also talks about the rights and duties of a data principal. Data principal has the right to access information about personal data (section 11), the right to correct and ensure personal data (section 12), the right to grievance redressal (section 13) right to nominate (section 14). According to Section 15.
A Data Principal shall perform the following duties, namely:—

(a) Comply with the provisions of all applicable laws for the time being in force while exercising rights under the provisions of this Act;

(b) To ensure not to impersonate another person while providing her personal data for a specified purpose;

(c) To ensure not to suppress any material information while providing her

Personal data for any document, unique identifier, proof of identity, or proof of address Issued by the State or any of its instrumentalities;

(d) To ensure not to register a false or frivolous grievance or complaint with a data fiduciary or the Board; and

(e) To furnish only such information as is verifiably authentic, while exercising
The right to correction or erasure under the provisions of this Act or the rules made there under.
This act also places several obligations on data fiduciaries Data fiduciaries will be obligated to maintain the accuracy of data, keep data secure, and delete data once its purpose has been met, etc . There is a very unique thing that makes The Digital Personal Data Protection Act, of 2023 special. That is this is the first Act of the Parliament of India where “she/her” pronouns were used unlike the usual “he/him” pronouns. This act specifies penalties for various offenses such as up to (i) Rs 200 crore for non-fulfillment of obligations for children, and (ii) Rs 250 crore for failure to take security measures to prevent data breaches. Penalties will be imposed by the Board after conducting an inquiry. If individuals want to file a case under the Digital Personal Data Protection Act, they can file a complaint with the Data Protection Board. If they are not satisfied then they can go to the Appellate Tribunal but even if they are not satisfied there, they can go to the Supreme Court. There is one major issue in this act the Act is only applicable to the data collected digitally and when offline data gets digitized. Not having the applicability on offline personal data.

Different case laws relating to data privacy in India

Here are some important case laws relating to data privacy in India:

1. MP Sharma v Satish Chandra(1954)

This was one of the first judgments of the Supreme Court relating to the right to privacy in India.MP Sharma v Satish Chandra case related to the search and seizure of documents of some Dalmia group companies following investigations into its affairs. Following an FIR, the District Magistrate issued warrants, and searches were consequently conducted. In writ petitions before the Supreme Court, the constitutional validity of the searches was challenged because they violated their fundamental rights under Articles 19(1)(f) and 20(3) — protection against self-incrimination. In M. P. Sharma vs. Satish Chandra, the 8-judge bench of the Supreme Court rejected the contention of the Petitioners that the right to acquire, hold, and dispose of the property was infringed upon by the search and seizure process. The Court observed that the act of searching did not deprive a person of the enjoyment of their property. The Court said that the Constitution of India did not have a fundamental right to privacy analogous to that of the Fourth Amendment of the US Constitution. The Court refused to import the principles of the Fourth Amendment in the form of the right to privacy.

1. Kharak Singh v State of Uttar Pradesh(1962)

The Kharak Singh vs State of UP case focused on the constitutional review of Uttar Pradesh Police Regulations, particularly Regulation 236. The right to privacy was invoked in this case to challenge the surveillance of an accused person by the police. Kharak Singh was arrested for dacoity but was released due to a lack of evidence. The Uttar Pradesh Police subsequently brought him under surveillance, which was allowed under Chapter XX of the Uttar Pradesh Police Regulations. Kharak Singh then challenged the constitutional validity of Chapter XX and the powers it conferred upon police officials, as it violated his fundamental rights under Article 19(1)(d) (right to freedom of movement) and Article 21 (protection of life and personal liberty). The 6-judge bench held that domiciliary visits at night were unconstitutional, but upheld the rest of the Regulations. More importantly, the bench held that the right to privacy is not a guaranteed right under the Constitution. As privacy continues to gain prominence in legal contexts, the foundation of arguments reflects the continuing quest for a balance between security and personal freedom.

1. Govind v State of Madhya Pradesh (1975)

In this case, a three-judge Bench of the Supreme Court for the first time extensively discussed the right to privacy under Articles 19(1) (d) and 21 of the Constitution in the context of police surveillance. The Court dismissed the Petitioner’s first submission, as surveillance to prevent further commission of the offense was in furtherance of the objects of the Police Act. On the second question, the Court discussed the concept of privacy and personal liberty extensively.

1. Justice K.S. Puttaswamy v Union of India(2017)

Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017), also known as the Right to Privacy verdict, is a landmark decision of the Supreme Court of India, which holds that the right to privacy is protected as a fundamental right under Articles 14, 19 and 21 of the Constitution of India. On August 24th, 2017, a 9 Judge Bench of the Supreme Court delivered a unanimous verdict affirming that the Constitution of India guarantees each individual a fundamental right to privacy. Although unanimous, the verdict saw 6 separate concurring decisions. Chandrachud J authored the decision speaking for himself, Khehar R.K. Agarwal, and Abdul Nazeer JJ. The remaining 5 judges each wrote an individual concurring judgment

1. State of Maharashtra vs Anil Mahadeo Deshmukh (2018)

State of Maharashtra vs Anil Mahadis significant case in Indian data privacy law. Here The court ruled that The right to privacy is a fundamental right under Article 21 of the Constitution and the government must ensure that personal information is protected from unauthorized disclosure.

1. Facebook vs Union of India (2018)

Facebook vs Union of India (2018) is a landmark case in Indian data privacy law. The Indian government sought to link Aadhaar (a national biometric ID) with social media accounts to prevent fake accounts and ensure accountability. Facebook challenged this move, arguing that it would compromise user privacy. The court says that Linking Aadhaar with social media accounts is not mandatory and Facebook must ensure data protection and privacy for its users.

Conclusion

Data privacy is very important in this digital life. Every individual people should understand the importance of data privacy. It is very important for a healthy society cause it ensures our rights, and safeguards our personal information. Data privacy gives individual rights to their data. An individual can access, control, and share their data. If the data principal wants, they can ask the company to delete their data, but the company needs to do it. If the company doesn't do that the data principal can file a suit against them. 137 out of 194 countries had put in place legislation to secure the protection of data and privacy. And in the future data privacy is going to play an important role in our lives.