Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

The need to Protect Data and Privacy laws in India

Saachi Dhingra[a]

[a]Vivekananda Institute of Professional Studies, New Delhi, India

Received 18 July 2022; *Accepted* 16 August 2022; *Published* 18 August 2022

Data surrounds us with all the actions we take in our daily lives. A single word is also counted as data. Whether you're traveling, ordering food, or using transportation, we generate data knowingly or unknowingly. In the present world, where data drives growth, data has become extremely important. What's even more appealing is that we are not even aware of all the data possibilities. As technology advances, new applications emerge that further enhance the value of data in our lives. As the value of data continues to grow, protection of important data is necessary. Lawyers in every corner of the world struggle to reconcile old legal methods with the era of ridiculously invasive data theft we face. Protective measures are needed to give national citizens and Consumers deep confidence in government, businesses, and other private institutions.

Keywords: *data protection, privacy laws, technological advancements, consumers.*

WHAT IS DATA?

Section 2 (1) (o) of the Information Technology Act 2000 (known as the "IT Act") refers to "data" as, "*a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer*

printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."[1]

WHAT IS PERSONAL DATA?

Data or information that is relevant or personally identifiable to a particular individual. It contains elements related to a particular natural person. Personal information is something that can be reconfirmed to recognize a particular sole. A variety of personally identifiable aggregated knowledge is sometimes referred to as personal particulars. Individually identifiable knowledge includes names, addresses, email addresses, phone numbers, Aadhaar card numbers, IP addresses, or medical records from doctors and hospitals. Personal information represents great commercial value in the market, so personal information is traded by many companies for financial gain. As a result, several nations in the world have enacted laws to protect this private information. Through the years, the amount of information generated by people has grown in the exponent. Present-day businesses create prodigious value by analyzing the details we generate. However, the main issue in the future is the ability to control what data is generated and how it is accessed and processed.

Protection is the choice to be freed from abuse or maltreatment of one's character or to be left alone. The right of security is the choice to be freed from unjustifiable revelation, to maintain a life of solitude and freedom from the absurd interference of the general populace in matters with which society isn't truly concerned.[2] At the point when the information that must be remained careful gets into some inappropriate hands, terrible things can happen. An information break at an administration association for instance can place closely guarded secrets into the foe's hands. Security is definitely not another idea. Security's a customary legal idea and an attack of protection gives an entitlement to the person to guarantee misdeed-build harms.

[1] Information Technology Act, 2000 Section 2
[2] Strunter v Dispatch Printing Co, Ohio App 3d 377

WHAT IS DATA PILFERING?

Data Pilfering is when information is moved unlawfully from one PC to the next to acquire advantages or admittance to some exclusive and touchy data of individuals. It is observed as a genuine break of protection and information. The outcomes of information burglary can be extreme for organizations and people. Information is typically stolen using USB drives, emails, malware attacks, and remote sharing.

HOW DOES DATA THEFT HAPPEN?

A variety of methods are used to steal information. Most typically, it occurs because someone broke into a computer system and stole sensitive information, such as your Visa card or personal information, or because a company employee mishandled the information. Many different companies and groups hold your personal information in our increasingly digitised environment, including your government-managed retirement number, postage information, birthdate, and ledger data. Indeed, even with new innovative advances, digital hoodlums can adjust and track down ways of hacking into frameworks to take information, particularly retail organizations that house installment data. Most organizations have information break plans set up; however, numerous representatives don't realize they exist or are uncertain the plans will work. All organizations that handle delicate information must instruct and prepare representatives on the best way to deal with touchy information.

INDIAN LAWS THAT GOVERN DATA PROCESSING AND DATA PROTECTION:

The information technology legislation of 2000 and the information technology rules (reasonable security practices and procedures and sensitive personal data or information), which gave guidelines, are said to have created the current system for information insurance. In cases where a body corporate is negligent in adhering to and carrying out reasonable security practices and procedures and causes unjust misfortune or improper increase to any individual, such a body corporate will be held liable to pay damages via payment to the individual so impacted, as stated in Section 43A of the IT Act. Section_66A of this Act manages wholesale fraud and states that any individual who deceitfully or deceptively utilizes a computerized signature, secret phrase,

or some other remarkable ID component of any person other than himself/herself will be rebuffed with three years of detainment and also pay a fine of Rs.100000

According to Section 75 of the Information Technology Act, the provisions of the IT Act will apply to any offence or contradiction reported outside of India by a person if the proof or evidence supporting the offence or contradiction uses a computer, computer framework, or computer network located in India. The scope of Section 69 of the Information Technology Act of 2000 includes both interfering with and watching alongside decoding for key reasons behind investigating digital wrongdoings in India. Additionally, the government has provided information under this section of the Information Technology (Procedures and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009. Under section 69A of the IT Act, the Government has recommended the Information Technology (Procedures and Safeguards for Blocking for Access of Information) Rules, 2009, that arrangements with the obstructing of sites are necessary. Numerous locations that fall under this requirement have had their entrances impeded by the government. The 2011 IT regulations mandate that body corporates storing sensitive individual client data adhere to a predetermined standard of security for preventing information theft.

INDIAN JURISPRUDENCE ON PRIVACY AND DATA PROTECTION

Article 21 of the Indian Constitution states that "No person shall be deprived of his life or individual freedom unless in accordance with the system established by law." The "right to protection" is not, however, referred to as a fundamental right in the constitution. The legal executive has frequently heard this topic brought up, and the legal executive has formed several hypotheses based on a variety of circumstances. Regarding ***M. P. Sharma and Others. v Satish Chandra, District Magistrate, Delhi, and Others***, the question of whether the right to security is covered by Article 21 was raised. However, for this situation, Supreme Court abstained from giving the right to protection as a key right.

On account of ***R. Rajagopal and Anr. v State of Tamil Nadu***[3] Supreme court saw that "*The right to protection is implied justified by the life and freedom that Article 21 guarantees to its citizens. It is a "right to be not to mention*." A resident has the concession to shield the security of his own. The Supreme Court determined that "The right to protection is impliedly justified by the life and freedom that Article 21 gives to its inhabitants" as a result of the case ***R. Rajagopal and Anr. v State of Tamil Nadu***.[4] There is a "right to be silent" about it. A resident has a right to protect his own security.

We have, therefore, no hesitancy in holding that right to security is a piece of the right to "life" and "individual freedom" protected under Article 21 of the Constitution, the Supreme Court stated in ***People's Union for Civil Liberties (PUCL) v Union of India***. Article 21 is invoked when actual circumstances in a particular situation establish a right to security. The aforementioned right cannot be restricted "other than as provided by methodology established by law. In one of the landmark rulings, ***K. S. Puttaswamy (Retd.) v Union of India***, this issue was raised once more. The court, in this case, stated that "*privacy is an innately guarded right that flows fundamentally from the provision of life and individual freedom in Article 21 of the Constitution*." Additionally, components of protection emerge in various contexts from various characteristics of opportunity and poise observed and guaranteed by the main privileges mentioned in Part III.

This ruling represents the biggest step away from acknowledging that the right to privacy is a fundamental freedom. We are definitely on the right track to establishing a framework that is designed to prevent the theft of personal information since the legal system views the right to security as a key right. As a result of this decision, many things, including "Aadhar cards," are now scrutinized and ensured that the important information of individuals is kept hidden and free from any breaches. Information is also evaluated and maintained carefully at many other government offices, which is a significant improvement.

[3] R Rajagopal and Anr V State of Tamil Nadu 1995 AIR 264
[4] *Ibid*

PERSONAL DATA BILL PROTECTION ACT 2019

The Personal Data Protection Bill[5], a draught rule on data protection in India, was spurred by the decision in ***K. S. Puttaswamy (Retd.) v Union of India***. On December 11th, 2019, the measure was introduced in the lower house of Congress. Although Parliament has not yet approved it, it offers us some food for thought on the development of India's information security laws. This bill aims to regulate how government agencies and for-profit organizations with connections to both India and other countries should handle citizens' private information. Handling of Data may be permitted if the individual gives consent to do so, in the event of a health-related emergency, or by the State to benefit its citizens. The individual will have a few rights in relation to their information, such as the ability to request a modification or request access to information that has been stored with private aspects. The measure allows for exclusions in some types of information handling, including handling for official purposes, public safety, and so forth. Additionally, it makes it necessary to keep a copy of the material on Indian soil. A certain amount of fundamental personal data should be stored only in India.

The Bill establishes a public level Data Protection Authority (DPA) to supervise and command information trustees. If information guardians cannot agree to:

1. For information handling commitments, the DPA may penalise them under this Bill.
2. The directions provided by DPA;
3. The requirements for cross-line information storage and movement. Failure to promptly inform the DPA may result in a fine of more than 5 crore rupees.

Additionally, anyone found guilty of disclosing, obtaining, moving, or offering to sell personally sensitive information faces up to a five-year prison sentence or a fine of three lakh rupees.

EVALUATION OF DATA PROTECTION ACT 2019

Although the measure includes considerable escape clauses, it still provides a basic framework for information insurance and efforts to protect information. The Data Protection Bill requires

[5] Personal Data Protection Bill 2019

information trustees to collect information in a reasonable and sensible manner that considers the security of the individual. However, the bill doesn't explicitly state or define what constitutes a reasonable and sensible way of handling individual information, which could lead to a shift in reasonableness and sensibility standards among information trustees handling similar types of information and in similar business activities. Before imposing information restrictions, India must also contribute to and develop the Internet network, server farm foundation, and matrix limit that are already in place in the nation. This will make it possible in any case for smaller organisations to comply with the information restriction.

The Data Trustee is given an optional power under the Bill to detail information breaks and determine if the information break has resulted in any harm to the Information Chief. When an information breach contains a small amount of a person's personal information, this may lead to careful disclosure of information breaches by information guardians, preventing the DPA from being triggered in any case. The Bill also doesn't take into account the semantics of a few key phrases. Information that is "serving duplicate" implies that it is dubious. Furthermore, it isn't immediately clear what is included in the definition of "basic individual information." The preparation of storing this information only within the territory of India is a crucial requirement for information guardians.

CONCLUSION

Every person on earth is aware of the need for information insurance legislation. Individuals require protection for their private, sensitive data. As a result, data assurance laws are becoming more popular worldwide. People are trying to get the government to follow more modern information insurance rules that allow people more transparency and protection of their own sensitive information. The Indian System is working to enact legislation governing information assurance, and a draught bill has already been created. It is, however, imperative that this bill be brought before parliament and scheduled as soon as possible.

While we may enact regulations across the country, it is also essential that the populace as a whole be "information sensitive," or aware of how their information is used by numerous

companies for their financial gain. With technological improvements, it will also be crucial for us to regularly update these information assurance rules while maintaining their unbending nature. After reviewing regulations from other countries, I believe the European GDPR establishes a gold standard for data protection laws.

Additionally, it levies stiff penalties against businesses that fail to take the necessary precautions to protect the information of its citizens. While there are many countries with approved legislation for information security and insurance, many other nations still do not have a regulation for the protection of their citizens' personal information. It is undoubtedly the ideal time for these countries to create and implement information security regulations. The guidelines now provided by the IT Act are undoubtedly insufficient for people in India. India has a big population, making it difficult to manage all of the information generated by the citizens. When there are information leaks, regular India should ensure the security of its citizens' private information by passing laws that are completely protected from the threats posed by modern innovations. All partners must align their agreements with the requirements of data protection, activate privacy reception, and investigate any potential consent requirements at the time of information collection in order for the information insurance system to be successfully implemented.