DATA PRIVACY & PROTECTION LAWS IN INDIA-A CRITICAL STUDY

Written by ***Jenifer Stella S* & Dr. Ambika Kumari S*****

**Research Scholar, Vel's Institute of Science Technology and Advanced Studies, Chennai, Tamil Nadu, India*

*** Professor and Dean, School of Law, Vels Institute of Science, Technology & Advanced Studies, Chennai, India*

ABSTRACT

This paper deals with the laws relating to protection of our data in the cyberspace. Cyberspace is an area that is promptly developing and has become a house hold need of every person in our day to day activities. All types of commercial and personal activities are been conducted online. We all have a parallel life in the cyberspace. Nowadays we have access to any data or information related to anybody from anyplace whenever we require. This emergence of technology has also given rise to e-danger to our personal and confidential information. Globalization has given acknowledgment of innovation in the entire world, according to developing prerequisite of various nations. Depending upon the usages of internet and the amount of data stored and transmitted online needs to be protected with proper legislation. The author shall highlight various issues and challenges faced these days in the protection of the data and the existing provisions dealing with data protection along with the need of specific data protection laws in India.

***Keywords*:** Cyber Space, Data, Information, Privacy, Protection, Legislations.

INTRODUCTION

As we live in a world which is advanced in technologies in various forms in both private and public activities and requirements. It is also the duty of the state to provide relevant laws and regulations to protect our data. Data protection can read as the set of rules, regulations and privacy policies of the country that intends to abate the use of personal information of any individual. Making the work of its people and general public easy technology is now being used to collect personal information for the functioning of either private or public organizations. The Constitution of India though not expressly clear on privacy as a fundamental right, however under article 19 & 21 of the constitution courts have guaranteed right to privacy. The Honorable Supreme Court in Puttaswamy (Retd.) & Anr Vs Union of India and Ors.[i] , held that right to privacy is protected as a fundamental right under Articles 14, 19 and 21 of the India.[ii]

DATA PRIVACY -NEED & SIGNIFICANCE

Data privacy or information privacy, can be understood as an area of which the prime focus is to maintain and protect the data which is considered to be sensitive in nature. Data privacy is just not the security and protection of personal data but is far more than it. It is an obligation on the part of the organizations to manage the personal data in a legitimate and ethical manner, this means that without the consent of the owner, their data should not be shared with the third parties. It owes a duty on the concerned organizations to be careful and clear with their customers on the data being collected and the purpose of utilizing those data. Though organizations recognize data breaches and are very well aware of the substantial threat of cyber-attacks yet they are negligent on the requirement to safeguard which is referred to as the "rights and freedoms of individuals". The organizations may retain the personal data of its customer, maintain it private in such a manner that it will not disclose the identity of the customers at the same time the reputation of the organization will also be protected A data breach at a government agency, corporation, school or hospital may put secret information's, proprietary data, students or patients information's into the criminal hands who could commit identity theft.

DIFFERENCE BETWEEN PERSONAL AND SENSITIVE PERSONAL DATA

Personal Data

Personal data can be distinguished as those information which helps to provide the identity of a person. This may include the name of the person, his account number or by other digital ways like the IP address of his system, his GPS or the username etc.

Sensitive Personal Data

Sensitive personal data can be understood as those information which may cause damage to an individual in case it is disclosed or mishandled. Following are few examples of Sensitive personal data:

- Racial or ethnic origin .Political or religious beliefs, Trade union membership ,Physical or mental health ,Sex life or sexual orientation ,Criminal offences and court proceedings, Voice recording, Health records, Political affiliations, Biometrics.[iii]

It is essential to understand the difference amongst personal data and sensitive personal data as extra care is required while handling sensitive personal data.

PROCESSORS VS CONTROLLERS

Controllers: The data controller determines the purposes for which and the means by which personal data is processed. This means that they make decisions about what information is captured and why?[iv]

Processors: The data processor processes personal data only on behalf of the controller. The data processor is usually a third party external to the company.

If a processor subcontracts some or all of the processing to another organization, the latter is referred to as a sub-processor.[v]

DATA CONTROLLER

I'm eventually responsible for my own compliance and the compliance of my processors. My duties incorporate compliance with information assurance standards, reacting to people's privileges, upholding safety efforts, overseeing information penetrates and connecting just with processors giving adequate protection to the data.

PROCESSOR

I have less self-governance over the information I am preparing, however I may in any case have direct lawful commitments. On the off chance that I connect with a sub-processor, I might be obligated to the controller for the sub processor's compliance. My obligations incorporate consistence with your controller guidelines as set out in outsider agreements, implementing safety efforts, advising controller of individual information penetrates and not connecting any sub-processor before the endorsement of the controller.

Sub-processor

I might be responsible for any harm brought about by my preparing on the off chance that I have not conformed to my legitimate commitments and in the event that I neglected to adhere to the Controllers instruction. My obligations towards the processor are like the processor's duties towards the Controller.

Persons' rights

The point behind protection laws is to empower individual and give them control over their own personal information.

Most data privacy laws acquaint what are generally alluded with as 'data subject rights' concerning the protection of individuals' personal data. It's imperative to take note of that not all of these rights are 'absolute', meaning some only apply in explicit circumstances:

RIGHT

- To access personal information: Individuals reserve the privilege to access and demand duplicates of their own information.
- Related to auto- dynamic and profiling: Individuals can protest choices made about them dependent on mechanized and mechanical handling.
- To object: Individuals can object to the processing of their personal information by an organization.
- To transfer personal information: Individuals can get data in a coordinated, ordinarily utilized machine-clear structure format.
- To address individual information: Individuals can have their own information corrected if erroneous, or complete if any incomplete.
- To erasure: Individuals can have their personal information deleted immediately
- To limit personal data processing: Individuals have the right to request the restriction of the processing of their personal information.

Processing of Personal Data

All information should be processed as per law. Organizations should have one of the below valid lawful bases for processing:

- Consent: of the person to the handling of their own information.
- Legitimate interest: of the association or the outsiders engaged.
- Contractual need: handling is required to go into or play out an agreement.
- Legal commitment: for which the association is obliged to deal with individual information for.
- Vital interest: of people, where handling is important to ensure their lives.

- Public interest: explicit to associations practicing official power or doing assignments in the public interest.

Data privacy laws indicate different conditions for processing sensitive and criminal information. Sensitive information can generally just be handled with the person's express assent, except if the information is needed for documenting legitimate continuing or claims, or if there is any lawful, public interest or administrative prerequisite. Individual information identifying with feelings and criminal offenses can typically just is prepared as long as it is completed heavily influenced by a specific government authority or as per neighbourhood laws.

LAWS ON DATA PRIVACY IN INDIA

Information Technology Act, 2000(Amendment Act 2008)

- **Section 43A: Compensation for failure to protect data**

  Under Section 43A of the IT Act, 2000, it is clearly stated that any corporate that possesses or handles any data which is sensitive in nature or any information contained and is in the control in its computer resource is found to be negligent in maintaining and applying rational care in providing security procedures which leads to any kind of damage to the person such corporate shall be liable to pay compensation, which may not exceed fie crore rupees.

- **Section 65:Tampering with Computer Source Documents**

  According to Section 65 if any person purposely hides, damages or modifies or intentionally makes somebody else to do the same with the computer system, computer programme or its network, when there is an obligation by law to maintain the computer

source code shall be punishable with imprisonment which may go up to three years, or wit fine up to two lakh rupees or both.

- **Section 66:Computer Related Offences**

  Section 66 states that if any person fraudulently indulges into any act which is referred in in section 43, shall be punished with imprisonment up to three years or with fine which may go up to rupees five lakh or both.

- **Section 66C: Punishment for identity theft.**

  As per section 66C if any person knowingly and dishonestly tries to copy and use the unique identification details of a person for example password or digital signature, shall be punishable with imprisonment for a term up to three years and fine which may go up to one lakh rupees.

- **Section 69 : Powers to issue directions for interception or monitoring or decryption of any information through any computer resource**

  Section 69 of the Act, directs the appropriate government to intercept or decrypt any information that is generated, stored or transmitted in any computer system. It means that government has been empowered to collect any information from any computer resource if it is found that such information might disturb the national pace and security or may violate any law.

- **Section 69 A: Power to issue directions for blocking for public access of any information through any computer resource**

  (1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government

or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.[vi]

- **Section 72: Breach of confidentiality and privacy**

According to 72 if any person has gained access to any type of electronic record such as a register, book etc and has disclosed information of such electronic records without the consent or knowledge or the owner shall be punishable with imprisonment up to for a term of two years, or fine up to to one lakh rupees, or both.

- **Section72 A: Punishment for Disclosure of information in breach of lawful contract**

Section 72 A brings an obligation on the intermediaries that when any information is collected as per the directions by law and without the consent of the owner, is knowingly used for unlawful purpose shall be punishable with imprisonment up to three years, or fine up to rupees five lakh , or both.

DATA PROTECTION IN OTHER COUNTRIES

Indian law on Data protection when compared with and the laws of developed nations the appropriate prerequisite required by the Indian law can be listed. Data Protection Act, 1998, is available in the United Kingdom. Data Protection Act is fundamentally founded to give both privacy as well as protection to the distinct information of the people in United Kingdom. According to the given Act, an individual or company that collects the information of individual should register with the information commissioner, who has been delegated as

public authority official to supervise the Act. This Act provides some restrictions on the collection of information. The information of an individual so collected will be satisfactory, applicable, and shall not be inflated according to the object for which they are handled.

Both the United States and the European Union emphasis on upgrading security assurance of their residents, Compared to European Union. U.S adopts an alternate strategy of protection. The United States included the sectorial method that counts on blends in the legislations, guideline, and other self-regulations. In United States, information usually are assembled in a few classes which is based on their utility and significance. From there on, in like manner an alternate level of security is granted to the various classes of information. While the IT Act manages extraction of information, annihilation of information, and so on Organizations can't get complete protection of information through which they are eventually constrained to go into discrete private agreements to keep the information secured. Such agreements shall have a similar enforceable procedure as the overall agreement.

The EU has authorized to all the members of its country a comprehensive Directive on Protection of personal data. The US & EU have consented to work together through the Safe Harbor Agreement. Indian shall also act wise and agree the mandates of the EU, as it also has a bundle in question.

Regardless of the endeavors being made for having an information insurance law as a different control, there are few lacuna in the bill of 2006. The drafting of the bill has been designed based on the United Kingdom’s Data Protection Act while the present necessity is of an extensive Act. Along in these lines it tends to be proposed that a gathered drafting based on US laws identifying with information insurance would be more great for the today' requirement. The actual requirement for the Indian Law can be examined on contrasting with the laws of India with those of the developed nations. UK’sData Protection Act, 1998 is fundamentally initiated to give security and protection of the individual information of the people in UK.

CONCLUSION

It is high time that India should have its own law on data protection laws that will ensure privileges of information which will restrict the utilization of the data collected and information gathered for such other purpose other than for which it was collected. The IT Act of 2000 cannot be regarded as data privacy or information protection legislation. The Act does not contains any particular information privacy or protection standards. The scope of the IT Act, 2000 is nonexclusive as it is focused on e-governance, electronic signatures, key infrastructure and cybercrimes. It will not be sufficient to compare the IT Act, 2000 with the laws of the other developed countries discussed above

India is lacking in specific legislations on Data protection law is enormous hit to rethinking on the privacy of its citizens. The clients of EU & US are ensured with a complete security command, and partially the it is required that the necessity of the security protection put on organizations, not to move data of an individual to those countries that bargain on a sufficient degree of assurance. The outcome is that European Trades Unions have referred to information insurance as an issue which ought to be considered in numerous global out-sourcing bargains. Its high time India requires a comprehensive legislation on Data Protection as compared to other developed countries to store and transmit sensitive information's.

REFERENCES

1. Phil Mennie,Richard Chudzynski , 2020, Data Privacy Handbook -A starter guide to data privacy compliance,.
2. The Information Technology Act,2000(Amendment Act 2008)
3. Peter Carey, 2020, Data Protection- A Practical Guide to UK Law.
4. Elif Kiesow Cortez,2021, Data Protection Around the World Privacy Laws in Action
5. Daniel J. Solove, Paul M. Schwartz, 2020, Consumer Privacy and Data Protection, Third Edition.
6. Lee Andrew Bygrave,2014, Data Privacy Law: An International Perspective, Oxford Scholarship Online, ISBN-13: 9780199675555

ENDNOTES

[i] (2017) 10 SCC 1
[ii] Bhandari, Vrinda; Kak, Amba; Parsheera, Smriti; Rahman, Faiza. "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict". IndraStra Global. 003: 004. ISSN 2381-3652
[iii] Available at https://www.pwc.com/m1/en/services/assurance/risk-assurance/documents/data-privacy-egypt-what-you-need-know-en.pdf
[iv] Ibid
[v] Ibid
[vi] The Information Technology Act,2000(Amendment Act 2008)