WILL – DATA PROTECTION LAWS IN INDIA

Why Does India Not Have A Data Protection Law?

Background

In essence, the Data Protection Bill 2019 sought to safeguard people's personal information and their right to privacy by enacting regulations to monitor how personal data is processed, as well as providing remedies or penalties for those who have been harmed by data breaches, unlawful processing of data, etc. According to the Bill, 'personal data' is any data about or relating to a person, who is directly or indirectly identifiable, whether online or offline, and shall include any inference drawn from such data for the purpose of profiling. It also categorizes certain personal data sensitive personal data including financial, biometric, caste, and religious information.

The Bill proposed the creation of a Data Protection Authority, a government-established, singular data protection body. This proposed authority would look into breaches of personal data, ensure compliance of data fiduciary, and ensure compliance of such fiduciaries with the Bill. In general, the Bill suggested limitations on the use of personal data without the citizens' consent. In terms of data processing, the Bill suggested a system that would control, among other things, cross-border data transfers and the accountability of data fiduciaries handling such data.

Big technology companies like Meta and Google were concerned about the Bill because they thought it may increase their compliance burden, increase their data storage needs, and impede cross-border data flow. For startups, it also made compliance more difficult.

On Wednesday, 3rd August 2022, The Government of India withdrew the Personal Data Protection Bill 2019 from the Parliament, while promising to come back with a new draft. IT (Information Technology) Minister Ashwini Vaishnaw said the bill was withdrawn because the panel suggested 81 amendments and 12 major recommendations.

In India, like any other rapidly developing nation, where the IT industry is expanding quickly, a Data Protection Act has long been overdue. According to Dutch cybersecurity firm Surfshark VPN, India has had the second highest number of data breaches in the first half of 2022. Keeping this in mind, India is in need of a concrete set of guidelines which lays down a clear-cut skeleton of compliances, rules and laws that binds any company or entity that deals with data. These laws will guide, warn and ensure that such entities follow the law and compliances and prevent any breach of data, uphold the privacy of users and minimize any risks that may occur while dealing with data in general.

The existing legal vacuum on data protection is an infringement of the fundamental right to privacy due to the lack of clarity on the laws regarding the same. It is necessary that

India forms a new law which is in line with all the advanced legislations related to data protection and privacy around the world in order to keep up with the progressing and advancing technology around the globe.

Data Privacy Laws That India Deserves

A case is sought to be made out which incorporates the following aspects in the Data Privacy Laws.

a) India's new law should separate personal data and non-personal data. Personal data is data about an individual or which relates to one, for example, our name, phone number, chat history, credit history, profile details etc. Non-Personal Data is electronic data that does not contain any information that can be used to identify a natural person. This will provide clarity and highlight the protection of extremely important data which is personal data. India currently lacks any sound legislation that safeguards personal data from any kind of misuse or illegal use. With the withdrawal of the Data Protection Bill, 2019, India needs a sturdy legislation addressing this issue.

b) India also needs guidelines that deal with cross border data transfer. With expansion in technology and opportunities, many Indian companies are dealing and working with international companies wherein personal data is involved, such as in new social media apps. Such initiatives involve data continuously being transmitted around the world, which is why rigid laws are required to regulate the same.

c) Moreover, data privacy laws should also incorporate regulatory guidelines with respect to internal transfer of data. The scope of the same can include legal ways to transfer data, penalties for offences committed related to transfer of data and other laws as required concerning the same.

d) Data privacy and data in general is always evolving in terms of its scope which is ever-expanding and its uses which are unlimited. Therefore, any legislation that comes about will need to be malleable around the developments that may take place in the future concerning data privacy.

In conclusion, data privacy rules are crucial in the modern era, when information and technology permeates every aspect of human life. Therefore, a country like India that is developing quickly needs a regulatory system and stringent laws that limit data-related offences and streamlines data related activities.

Dr. Pallavi Divekar