Webology (ISSN: 1735-188X)
Volume 18, Number 5, 2021

Data Protection Laws: A Global Outlook

Dr. Sanchita Ray[1] , Dr. Sanskriti Mishra[2] , Snigdha Kuriyal[3] , Bhumika Sharma[4] , Priti Chaudhri[5]

[1]School of Law, Sharda University, Knowledge Park -III, Greater Noida, India.

[2]School of Law, Sharda University, Knowledge Park -III, Greater Noida, India.

[3]ICFAI Law School, ICFAI University Dehradun, India.

[4]Jagran School of Law, Selaqui, Dehradun, India. https://orcid.org/0000-0002-3963-6036

[5]School of Law, Sharda University, Knowledge Park -III, Greater Noida, India 2020466333.

Abstract

Hunger for power has led to two World Wars which resulted in huge loss of life and property. Now, it is the hunger for information, which is causing severe damage, in terms of economy, political and social, to several states around the globe. This hunger for information has given birth to cybercrimes, fermenting of privacy, etc. Cybercrimes are committed in or through the medium of internet, some of the examples are theft, mischief, cheating, fraud, misrepresentation, pornography, intimidation, threats etc. They have posed a potential threat to the business houses, financial institutions, and the governmental bodies. So, at present it became pertinent to give adequate protection to huge databases so as to stop cybercrimes. But due to the absence of stringent laws relating to data protection, the cybercrimes are increasing day by day. New laws should be made in consonance with the present and future technologies which can strictly handle cybercrimes. Patchwork of law dealing with data protection lacks efficiency and effectiveness. With a recent rapid increase in infringement on privacy information, a need to protect privacy information is called for more than ever. In the present times of massive data breaches, if India lags in a sound and secure data protection regime, this will massively hamper its position on the global commercial map. Hence, a rehauling of the data protection regime is very much needed. This paper discusses various laws enacted in India, to deal with protection of data and compares laws of other countries. Further, this article highlights the various loopholes that exist in relevant provisions dealing with data protection in India.

Keywords – Data; Globe; Information; Technology; India.

INTRODUCTION

Maintaining of data bases is not as much difficult task as maintaining its integrity, so in this era the most concerned debate is going on to innovate a perfect method of data protection. In the present era most of the crimes are being done by the professionals through the easiest medium i.e. computers and electronic gadgets. Just by the single click, the criminals are able to get the secured information. The lust of information is acting as a catalyst in the growth of cybercrimes. It is the very big headache for the business houses, financial institutions and the governmental bodies so as to give adequate protection to their huge databases. In the absence of any particular stringent law relating to data protection, the miscreants are gaining expertise in their work day by day.

Many countries other than India have their data protection laws as a separate discipline. They have well framed and established laws, exclusively for the data protection. When we analyse the data protection laws in India and the European countries, it is found that a couple of loopholes exists. The very obvious difference is the absence of a dedicated and comprehensive data protection legislation in India. Despite the efforts being made for having a data protection law as a separate discipline, our legislature has left some lacuna in framing the Bill of 2006. Moreover, the provisions of information technology act deal basically with extraction of data, destruction of data. Companies cannot get full protection of data through that ultimate forced them to enter into separate private contracts to keep their data secured. These contracts have the same enforceability as the general contract.

Even though India does have provisions under the different acts, it lacks efficiency and effectiveness due to the absence of dedicated and detailed framework to address the issue. With a recent rapid increase in infringement on privacy information, a need to protect privacy information is called for more than ever. The U.S has adopted a sectoral approach to make data protection more efficient by regulating the flow on a data protection sector- to- sector basis.

METHODS

The research methodology adopted and applied by the researchers in this research study is basically doctrinal. The tools of data collection are books upon the subject of eminent writers and scholars, available in various libraries and other places; the reports of the various government authorities as well as special reports of the special committees and commissions constituted by the government of India or the State government (if any); reports of the non-governmental organizations; scholarly articles on the subject of this research written by various scholars in different law journals, magazines, newspapers and websites. The paper also used relevant the legislative provisions, international instruments, etc.

RESULTS & DISCUSSIONS

This Part of the Paper shall discuss and analyse the features of the data protection in India and Europe. It also points the loopholes in the Indian legal framework regarding to data protection:

LOOPHOLES UNDER INDIAN LAWS: THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 does not contain a definition of 'data breach'. Data breach issues have been increasing day by day, the need for dedicated legislation also increases. Moreover, the terms and provisions are very ambiguous. For example, there is no clear demarcation between 'personal' and 'sensitive' information. Also, the term 'data' under the information technology act, 2000 is only restricted to computer – based data. In 2015, in the case of Shreya Singhal vs. Union of India (AIR 2015 SC 1523), Section 66A of the Information Technology Act was struck down on the grounds that it was vague.

The provisions of the act only deal with the collection and distribution of information by a body corporate. The term consent has not been defined under the act. Another issue with the Indian laws is the inadequacy and sufficiency of penalties. The penalties are mostly monetary in nature, which fails to have a deterrent effect. However, when we look at the European Union's general data protection regulation (GDPR), despite a few loopholes, it is effective as it is concise, and directly address the issue at hand. The high fines and stringent punishments help as a deterrent to future offences. (Information Technology Act, 2000, Section 43A, 72, 72A)

Privacy Policy: The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 provide for formulation of a privacy policy by body corporates dealing with personal data. Such privacy policy should contain the following:

- Statements of its practices and policies. Such statements should not be ambiguous and should be easily accessible.
- Purpose for which data is being collected.
- Type of personal or sensitive personal data being collected.
- Disclosure of information
- Reasonable security practices and procedures.

Non- disclosure of personal data to the third party: The collectors of data are mandated not to disclose the personal data collected in accordance with the SPDI Rules India to third parties, without the consent of the provider of the data. (The Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011). However, a disclosure mandated under law is outside its scope.

Transfer of data: The data collected can be transferred to a third party with the prior consent. Such third party may be located in India or abroad. Care needs to be taken that such third party is complying with and implementing similar data protection mechanisms as deployed by the transferor of the data.

Personal Data Protection Bill: It is important to note that there is no specific data protection legislation in India. The Personal Data Protection Bill, 2006, was introduced in the Rajya Sabha in 2006 with the goal of protecting an individual's personal data and information collected for a specific purpose by an organization and preventing its use by other organizations for commercial

or other purposes. Following the Supreme Court's decision in the landmark Right to Privacy Matter, Justice K.S. Puttaswamy v. Union of India, (AIR 2017 SC 4161) which declared the right to privacy to be a fundamental right, it was felt that it was critical to protect personal data as a facet of informational privacy. According to the Justice Srikrishna Committee's recommendations (Report on A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, 2018), courts of law and regulatory authorities should be allowed to develop principles of fair and reasonable data processing. The Bill requires data fiduciaries to collect data in a fair and reasonable manner that respects individuals' privacy, but it does not explicitly specify a fair and reasonable manner of personal data processing, which could result in fairness and reasonability principles varying across fiduciaries processing similar types of data and fiduciaries in the same business evolving an approach.

As a result, the Personal Data Protection Bill, 2019 was introduced in Parliament, with provisions covering various aspects of data protection. This Bill was referred to a Joint Parliamentary Committee of both the Houses for examination and Report in February, 2020. The Joint Parliamentary Committee (JPC) released its much-awaited report on the Personal Data Protection Bill, 2019 in December 2021. (P.P. Chaudhary, Joint Committee on the Personal Data Protection Bill, 2019, 2021)

Simultaneously, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, require 'publishers' to, among other things, append declarations of compliance in the terms and conditions or privacy policy displayed on their website. Businesses are, therefore, required to develop robust interconnected frameworks for compliance with the information security and privacy laws. Though India's existing laws do not provide the necessary data protection, the country is in the process of drafting a data protection legislative enactment.

General Data Protection Regulation: GDPR Regulations are primarily focused on protecting personal data. Personal data is defined as any information which helps in identifying an individual. Hence, even particulars like name, contact details, addresses etc. would constitute personal data. The party which determines how the data is to be used is the data controller, the party which processes is the data processor and the provider of information is the data subject. (GDPR, Article 4).

European Union has come up with a new set of data privacy norms which are bound to have far-reaching effects. In the wake of data security breaches by big players such as Facebook, Paytm and Google, GDPR appears to be a strong step taken by the EU towards the maintenance of data security it is high time for Indian lawmakers to evaluate whether our extent data protection regime is adequate to address the challenges posed by the ever- growing transparent world. The following are the key features of GDPR Regulations:

- Accountability: The GDPR Regulations have introduced a two-pronged accountability system, wherein both the data controllers and the data processor are accountable for any

kind of data breach. Both data controllers and processors are required to maintain data processing registers.

- Consent: GDPR takes into account only freely given, specific and unambiguous consent. It also enables the data subject to withdraw his/her consent.
- Breach notification: GDPR Regulations require that any data breach should be notified to the data subject within 72 hours of the occurrence of such breach.
- Access: The Data Subject is entitled to request access to the data and information pertaining to the manner of processing and the purpose for which it is being processed.
- Right to be forgotten: Upon data subject's request, the company is obliged to delete all the data stored. This generally happens when the data is no longer relevant.

Data Protection Officers: The GDPR requires the appointment of data protection officers by companies having 250 or more employees or 5000 or more data subjects.

Comparative Analysis: On comparing the Indian law with the law of developed countries like the UK, the US, and the European Union countries the proper requirement for the Indian law can be analyzed. We find that all the developed countries have their personalized strategies for addressing their data privacy issues. Each country has endorsed a separate approach to enact the data protection laws, after considering the utility value in their country, as data are not of same utility and importance; it varies from one another on the basis of utility.
GDPR has 3 objectives broadly which are "protection of natural persons when their data is processed, protection of their fundamental rights and freedoms with respect to data protection and freedom of movement of personal data for processing purpose. The Regulation confers protection to data subject as a matter of right". Additionally, GDPR reaffirms the rights granted by the Charter of Fundamental Right of European Union and Treaty on functioning of European Union.

Section 43A of the IT Act gives an insight about the objective of IT Act and rules which is to provide a model law to assist e-commerce in a smooth manner. Both regulations strive to promote a transfer of data for encouraging e-commerce. Though, GDPR is a step ahead as it not only intends to assist data transfer but also to protect the rights of the person throughout the processing of data. The principles of processing and collection of data is one head which grabbed the most attention during the framing of GDPR. The IT Act rules and GDPR both lay down the principle for data protection. The rule 5 of the IT act states that there should be lawful object behind collecting the information and should be with regard to doings of an enterprises for a time period required to fulfil the object to a collection in the first place. The data processing under GDPR is steered by "purpose, limitation, accuracy, storage limitation, integrity, confidentiality, and accountability." Both the laws have the same stand regarding the lawful objective behind the collection of data. Furthermore, The IT rules suggest that the data can't be retained for a longer period than required to achieve the object, the GDPR have some reservations on the same.

The difference lies in the fact that the term "processing" has been defined under Article4(2) of the GDPR but the term 'processing' as a definite, concrete term has not been defined at all under the

IT Act. Though a relation can be drawn by the usage of the word processing in definition of the term ‘Data. An inference can therefore be drawn that since the word ‘processing’ has been used in defining "data". Furthermore, data has been included while defining information, so, by applying the golden rule of interpretation, it could be said that the above-mentioned rules are also applicable to processing. However, GDPR takes another step by not only restricting the rules to a lawful purpose for data collection and retention but by supplementing them with rules pertaining to data integrity, transparency, fairness and safeguarding the data from illegal processing and damage, unlike IT Act.

Additionally, the fundamental of accountability is also a key feature of GDPR which makes the controller liable in case non-compliance with the principles of GDPR, the same can’t be said for IT rules. The accountability of the controller is nowhere expressly mentioned in the legislation but a circuitous reading of Rule 5, could make up for the gap. Oddly despite the lack of robust framework the IT rules has been quite comprehensive with the definitions by distinguishing between "sensitive data" and "information", both of them is governed by a separate set of rules. For instance, the rule that there must be a lawful purpose to collect information regarding the activities of the corporation, applies to "sensitive personal data", the same is not applicable to "information". Similarly, the purpose restriction stated under rule5 (5) applies to the "information collected", which doesn't include the "sensitive data" in its purview. The purpose behind this difference is still a mystery.

GDPR, on the other hand, is concerned with the processing of "personal data" in general. Another point of difference is that IT rule 5 is not applicable to “company collecting personal data under a contractual obligation with another Indian or foreign company”. This leads to an inference that the enterprises which directly get into a contractual obligation with natural persons to collect personal data are subjects of this principle, whereas the GDPR doesn't have any such stipulation.

India’s current data protection bill 2011 is inadequate to handle the kinds of threats that plague personal data today. As a first step, a dedicated data protection law should be enacted on the lines of the GDPR Regulations. The term ‘reasonable security practices and procedures’ should be clearly defined and maybe a sample policy mirroring the same may be framed by the government to serve as a reference point to the companies. Penalties should be increased in order to create a better deterrent effect.

The new law should be made in consonance with the present and future technologies. In the present times of massive data breaches, if India lags behind in a sound and secure data protection regime, this would massively hamper its position on the global commercial map. Hence, a rehauling of the data protection regime is very much the proverbial ‘need of the hour’. The IT act since it was not created with the intent of protecting consumer information, doesn’t have the same safeguards as GDPR. The courts through judicial interpretations can provide for regulation of data as well as processing.

It can be seen from the structure of GDPR and the fines which have been levied, that the European Union has given utmost priority in regulating and safeguarding the personal data of its citizens. GDPR ensures transparency and accountability. Stringent fines act as a deterrent for the organization to not neglect or compromise fulfilling their duties under GDPR (GDPR, Article 83).

With respect to the territorial scope, the PDPB's scope of application is potentially broader than that of GDPR, as an entity may fall within scope merely by processing personal data in India. However, the government has the authority to exempt any of such processing activities when required. The GDPR applies to Organizations that have an establishment in the European Union and process personal data "in the context of" the EU establishment.

Organizations that are not established in the EU but process personal data in relation to either (a) offering goods or services in the EU; or (b) monitoring the behavior of individuals in the EU. Whereas the PDPB applies to Processing personal data that has been collected, disclosed, shared or otherwise processed within the territory of India (S. 2(A) (a)). Indian companies, Indian citizens, and any other persons or bodies incorporated or created under Indian law (S. 2(A) (b)). Personal data is any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, taking into account "all of the means reasonably likely to be used."

Whereas in Personal Data Protection Bill, 2019, the Personal data is data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.

The Council of Europe Data Protection Convention of 1981 (usually referred to as Convention 108 or the COE Convention) is the most prominent binding international agreement on data protection. Although this Convention was established by the Council of Europe, its membership is open to any country, and several non-European countries have signed the Convention or are in the process of becoming members.

Forty-six of the forty-seven Council of Europe member States have ratified the Convention and have implemented data protection laws that comply with the Convention but with the exception is Turkey where ratification is in progress, the Turkish parliament has recently passed a data protection law. Uruguay was the first non-European country to become party to the Convention in 2013. Four other countries are currently exploring membership i.e., Mauritius, Morocco, Senegal and Tunisia. The Convention differs from many other global initiatives in that it is binding on signatories. (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,1981).

The definition of personal data under the PDPB is broader than the corresponding GDPR definition. The GDPR concept of personal data takes into account the reasonable likelihood that

an individual will be identifiable. This flexibility does not appear in the PDPB. Inferences are expressly within scope of the definition of personal data under the PDPB, where they are derived from personal data for profiling purposes. Under the GDPR, inferences may be personal data to the extent they relate to an identifiable individual, but not all inferences derived from personal data will also be personal data.

The compensation granted under the Data Protection Law may be on a per day basis on which the upper limit is fixed usually by the adjudication body, and that limit is at the depend on variable parameter. With regards to compensation for damages due to infringement of data protection, IT act and GDPR have adequate provisions under section 43A and Article 82 respectively. However, both legislations have granted some exemption from liability. According to the 82(2) of GDPR, the controller can escape the liability if he successfully proves that the infringement was beyond his control and he isn't responsible for the same.

Similarly, if the controller satisfies the conditions of implementing adequate security measures to protect the information, he too shall not be liable to pay compensation under the IT Act. The distinction between the laws lies in the nuances i.e. under the IT Act, the competent authority varies with the amount of compensation. For instance, the Section 46(1A), the adjudicating officers have the jurisdiction to entertain the dispute up to 5 crores only, for the dispute whose valuation exceeds this amount will have to approach the competent court.

On the contrary, GDPR has given the absolute power to the Member State's court to adjudicate the matter without any bar on the pecuniary jurisdiction, but it shall be done in accordance with the case laws as developed by the European Court of Justice. Another distinction lies in the fact that IT Act makes it difficult to make successful claims against privacy breach by mandating the requirement to establish that there had been an illegal loss or gain due to the breach, unlike the GDPR which doesn't require the aggrieved to prove mens rea, similarly information disclosure has grave repercussions under both the laws. Section 72A of IT Act imposes a fine up to 5 lakh INR whereas GDPR imposes an exemplary fine up to 10,000,000 EURO or 2% of total wide turnover of preceding financial year, whichever is higher.

Though, the difference between the two is that IT Act imposes criminal liability under Section 72A in case of breach of data confidentiality contract, unlike GDPR which doesn't impose criminal liability and rather resort to hefty administrative fines. There exists two-fold redressal mechanism under GDPR, the aggrieved could either file a complaint with a supervisory authority or he can approach the judiciary to get justice. Under GDPR, the data subject doesn't need to exhaust all his administrative remedies before approaching judiciary.

The IT Act puts the Adjudicating officer, designated by the enterprise, to redress the grievances related to processing of information. He has the power to investigate the matter and decide the quantum of compensation as well. An appeal against the adjudicating officer lies with the Cyber Appellate Tribunal. Despite clarifying the pecuniary jurisdiction of the adjudicating officer, the

competent court for matters above 5crores has not been stated for the purpose of filing a complaint under section 43A of the Act.

Further, the IT Act creates a criminal liability under section 72A for disclosure of lawful contract. It "falls short of creating a private right of action on behalf of individuals whose data is being handled by any third parties because it is still cast as a penal provision and does not create a private right of action in civil law…an individual cannot file a suit in civil court under this section as it does not create a statutory right to damages or compensation, that is, there is no private right of action for damages in civil law". Though, the procedure to approach in absence of civil court, to impose criminal liability is ambiguous.

In general, there is significant overlap between the way sensitive data is defined under each framework, but the definition of sensitive data is broader under the PDPB. The PDPB includes "financial data" within the scope of sensitive data. The PDPB allows the government to define additional categories of sensitive data, whereas the list of categories under the GDPR is finite. One exception is that the GDPR provides for additional rules for processing criminal convictions and offenses data, but the PDPB includes no similar provision.

There are certain provisions in the PDP Bill that matches with the provisions given in EU GDPR. It is worthy to mention here that the GDPR is considered one of the best models on personal data protection worldwide. However, PDP Bill differs from GDPR in some aspects. The PDP Bill differs from European Union with respect to the presence of provisions related to social media intermediaries and non- personal data. The comparison is shown in table presented below.

CONCLUSIONS

To sum up, similar legislation is needed in India. Personal data protection bill is required to be converted into an act as the current data protection bill is inadequate to handle the kinds of threats that plague personal data today. The new law should be made in consonance with the present and future technologies.

Though inspired in part by the EU General Data Protection Regulation, India has ultimately forged its own path toward data protection with several unique provisions: combining personal and non-personal data under the same umbrella, data localization, coverage of hardware devices, managing social media platforms, and more. Talking about the GDPR, in many cases, the scope is very rigid. The table depicts that as compared to GDPR less provisions to data subjects are available in India. Nonetheless, it is functioning well, even though the companies have definitely felt its impact where they had to revise their privacy policies and take consent of the data subject. With the recent news, where the EU denied former Facebook, presently meta, to process the data of the EU citizens after it was found that they were grossly misusing the data.

Overall, both the regulations are essential to regulate the processing and protection of data in these times where data collected are being misused and used for manipulation of various forms. In India, this Bill should come into effect as soon as possible because the personal information of the

citizens is at stake here. Though, India lacks exclusive legislation to protect personal data, the combination of the Information Technology Act, 2000 alongwith its Allied Rules definitely govern the data protection framework in India.

REFERENCES

1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,1981.
2. European Union General Data Protection Regulation, 2018
3. Information Technology Act, 2000 (India).
4. Justice B.N.. Srikrishna, Report on A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, 2018.
5. Justice K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.
6. P.P. Chaudhary, Joint Committee on the Personal Data Protection Bill, 2019, 2021.
7. Personal Data Protection Bill, 2019 (India).
8. Shreya Singhal vs. Union of India, AIR 2015 SC 1523.
9. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).