DATA PROTECTION LAWS IN INDIA AND EU GENERAL DATA PROTECTION REGULATION: A COMPARATIVE VIEW

-Shruti Sharma[1]

ABSTRACT

2018 was a big year for data privacy and data processing regulation. On July 27, 2018, India published a draft bill for a new, comprehensive data protection law to "be called the Personal Data Protection Act, 2018," only a few weeks after the European Union General Data Protection Regulation (GDPR) took effect on May 25. With the new law, the Indian government responds to a mandate from the Supreme Court of India, which had directed the government of India in August 2017 to enact comprehensive data protection legislation.

Presently, there is no specific legislation with dealing with privacy and data protection in India. The protection of privacy and data can be derived from various laws pertaining to information technology, intellectual property, crimes and contractual relations. However, presently the Information Technology Act, 2000 (the "IT Act") contains specific provisions intended to protect electronic data (including non-electronic records or information which are processed electronically).

India is still at a relatively nascent stage when it comes to data protection regulations, as compared to other jurisdictions such as the highly developed guidelines prescribed by the European Union ("**EU**") on data protection. Comparison of the two legal regimes offers certain interesting insights on data protection laws. The aim of this paper is to make a comparative analysis on existing right to privacy and data protection laws in India with the regulations of European Union General Data Protection Regulation (GDPR) took effect on May 25.

I. INTRODUCTION

Data is surrounding us and is present in everything we do. One is that we share on our own and the other is which is generated every time we do something starting from booking a flight ticket

[1] *Shruti Sharma is a student at Symbiosis Law College, Nagpur.*

to buying a food through Zomator or Swiggy. For these reasons data is very important and valuable for many companies in the following ways:

1. **Improving customer experience**: Using personal data companies can find out about the demand of customers.
2. **Refining marketing strategy**: Personal data helps to know about how customers are responding and engaging with their competitor's strategy.
3. **Turning data into cash flow**: Business companies which get hold of personal data sell it to other companies and make profit.

In the absence of any specific single piece of legislation, currently there are a number of legislations governing different aspects of data protection and security in India. The Information Technology Act 2000 is the primary law in India dealing with cybercrime and electronic commerce. It also contains provisions for the protection of electronic information. Besides these laws, there are a variety of laws in India which contain provisions dealing with the processing of data, which includes personal data as well as sensitive personal data. These laws include but are not limited to Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act"), The Indian Telegraph Act, 1885, Right to Information Act, 2005 and many more.

Similarly, companies all over world are in the process of assessing the impact that European Union(EU) General Data Protection Regulations ("GDPR") will have on their businesses. The European Union's (EU's) General Data Protection Regulation (GDPR) took effect on 25 May 2018, harmonizing data protection and privacy requirements across the EU known as the Regulation of the European Parliament and the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC ("**General Data Protection Regulation**" or "**Regulation**"). It is worth mentioning, that in accordance with Article 288 of the Treaty on the Functioning of the European Union, the Regulation is binding in its entirety and is directly applicable in all Member States of the EU. Therefore this Regulation does not require additional implementation of acts of national law, as the provisions included in it are binding from the date of its entry into force. Concern regarding non-compliance of GDPR and the loss of business is also a major issue for India. Existing literature on the GDPR suggests significant economic consequences for the EU, with a potential to impact small and medium-

sized enterprises (SMEs), labor markets, cross-border trade, and overall economic growth. A detailed analysis of the literature assessing the impact of the GDPR highlights both the potential negative consequences of a GDPR-like data protection law for India and the necessity of undertaking similar studies in India prior to the bill's implementation.

II. PERSONAL DATA AND ITS PRIVACY

The 21st century is known as information age. With computers and internet being the integral part of life of humans in this century, it has connected the world like never before. The individuals in general and the business in particular have benefited from the geography less environment where only the best can be purchased and only the best can be sold. In initial years business used this information only as data bases and were mainly used for statistical purposes. But in recent times the information is being converted into data (i.e. into a format which can be used for a specific purpose) into a matter of seconds. In fact these days an individual gives away data even without his own knowledge.

An act as simple as eating at restaurants, buying goods online or even hailing a taxi gives out precious data about oneself. All the transactions that we enter into using either smart-phones or the computers require individual to fill in personal data such as date of birth, age sex, residential address, phone numbers and financial information. This gives away information about individual choices about what colour one likes to wear, what size fits him/her, what food he/she like to eat etc. In other words an individual gives away his privacy even without his knowledge.

Businesses on the other hand are using this data for commercial purposes. The bombarding of advertisements about a product or services which you would have clicked upon while surfing through the internet hound you everywhere. Not just this there are websites, where if you have entered your date of birth and the size of dress that fits you, the website runs an algorithm by which it puts before you analysis about what your age is, your ideal weight, if you are near or far away from your healthy weight, what nutrition should you follow, exercise plan. It also would give you addresses of nutritionists and Gymnasiums near your area of residence.

Such kind of bombarding of information may not seem harmful in first instance but it definitely affects an individual's privacy. That is why economies all over the world are increasingly moving towards making laws that protect the privacy of individuals.

Sharing data may bring benefits, the products and services are tailor made thus reducing the time and effort one spends in identifying what suits them. But sharing of data it is not without risks. Your personal data reveals a lot about you, your thoughts, and your life. These data can easily be exploited to harm you, and that's especially dangerous for vulnerable individuals and communities, such as journalists, activists, human rights defenders, and members of oppressed and marginalized groups. That is why these data must be strictly protected. When data, which should be kept private gets in the wrong hands, bad things can happen. A data breach at a government agency can, for example, put top secret information in the hands of an enemy state. A breach at a corporation can put proprietary data in the hands of a competitor.

Realising the need to protect data, governments all over the world have taken measures to protect it. The government is entrusted with the task of protecting the business and allowing them freedom to do business and at the same time to ensure that privacy of individual is protected. The Right to Privacy stems from the constitutions in some countries for example European Union and India while it is ensured by various legislations in countries, like United States of America, Australia and China. For these reasons there have been different approaches around the world while dealing with Personal data protection regulations.

III. REGULATORY FRAMEWORK IN INDIA

(i) Information Technology Act, 2000 and SPDI Rules

In the absence of any specific single piece of legislation, currently there are a number of legislations governing different aspects of data protection and security in India. The Information Technology Act 2000 ("**IT Act**") is the primary law in India dealing with cybercrime and electronic commerce. It also contains provisions for the protection of electronic information. The IT Act also prescribes punishment of imprisonment and/or fine for offences involving illegal downloading, destruction, alteration or deletion of data, introduction of viruses into

computer systems, illegal access to computer systems, data theft, identity theft, cheating by personating, cyber terrorism, breach of confidentiality, privacy and disclosure of information in breach of lawful contract, to name a few.

Various Rules under the IT Act were also passed in April 2011, important among them being the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, which require entities holding users' sensitive personal information to maintain certain specified security standards ("**SPD Rules**").

(ii) The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act")

The Aadhaar Act enables the Government to collect identity information from citizens including their biometrics, issue a unique identification number or an Aadhaar Number on the basis of such biometric information, and thereafter provide targeted delivery of subsidies, benefits and services to them. The requesting entity (government/public and private entities/agencies) is required to obtain the consent of the individual before obtaining his identity information for the purpose of authentication and must use his identity information only for the purpose of authentication.

(iii) **Telecom Sector**

There are multiple laws that operate in the telecom sector such as the Indian Telegraph Act, 1885 (Telegraph Act), the Indian Wireless Telegraphy Act, 1933, the Telecom Regulatory Authority of India Act, 1997 (TRAI Act) and various regulations issued there under. A telecom service provider has an obligation to take necessary steps to safeguard the privacy and confidentiality of the information of individuals to whom it provides a service and from whom it has acquired such information by the virtue of the service provided.

(iv) Health Sector

The Clinical Establishments (Central Government) Rules, 2012 ("Clinical Establishments Rules") requires clinical establishments to maintain and provide Electronic Medical Records/Electronic Health Records, thus mandating the storage of health information in an electronic format. The SPDI Rules recognise health information as constituting "sensitive personal data" and thus regulates its collection, use and disclosure.

(v) Other legislations in India that impact Data Protection

Currently, there are a variety of laws in India which contain provisions dealing with the processing of data, which includes personal data as well as sensitive personal data. These laws include but are not limited to the following:

a) Banking Regulation Act, 1949
b) Credit Information Companies (Regulation) Act, 2005
c) Credit Information Companies Regulation, 2006
d) Reserve Bank of India Act, 1934 including Master Direction on Know Your Customer (KYC), 2016.
e) Right to Information Act, 2005

(vi) A New Data Protection Law on the Horizon

With the gamut of laws regulating collection and usage of various types of data, the data protection regime in India is still not exhaustive enough, and several concerns are being raised to further secure and adequately deal with the complex issues including loss of data and consequent privacy. A Committee of Experts under the Chairmanship of former Supreme Court Justice, Shri B. N. Srikrishna ("Committee) has released a white paper on November 27, 2017, on a data protection framework for India, seeking public comments. This white paper has come on the heels of the Supreme Court's landmark judgment of August 24, 2017 in the case of **Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., 2017 (10) SCALE 1,** where the Supreme Court has recognized right to privacy as fundamental right under Article 21 of Indian Constitution.

On the basis of the White Paper of the Committee, the Government proposed the draft "The Personal Data Protection Bill 2018" on 27th July 2018 to protect citizens' data and privacy, which is yet to be passed by the Parliament.

IV. REGULATORY FRAMEWORK IN EUROPEAN UNION

In April 2016, the European Parliament adopted the GDPR, replacing its outdated Data Protection Directive, enacted back in 1995. Unlike a regulation, a directive allows for each of the twenty-eight members of the EU to adopt and customize the law to the needs of its citizens, whereas a regulation requires its full adoption with no leeway by all 28 countries. In this instance, the GDPR requires all 28 countries of the EU to comply. The issue with the Directive is that it's no longer relevant to today's digital age. Its provisions fail to address how data is stored, collected, and transferred today—a digital age.

The full text of GDPR, which came into effect from 25 May 2018, is comprised of 99 Articles, setting out the rights of individuals and obligations placed on businesses that are subject to the regulation. GDPR's provisions also require that any personal data exported outside the EU is protected and regulated. For example, a Indian airline is selling services to someone out in the UK, although the airline is located in India, they are still required to comply with GDPR because of the European data being involved.

Two major protective rights under GDPR are:

(i) Right of erasure, or the right to be forgotten. If you don't want your data out there, then you have the right to request for its removal or erasure.

(ii) Right of portability. When it comes to "opt-in/opt-out" clauses, the notices to users must be very clear and precise as to its terms.

What happens if you fail to comply with GDPR? Just ask Facebook and Google who were hit with a collective $8.8 billion lawsuit (Facebook, 3.9 billion euro; Google, 3.7 billion euro) by

Austrian privacy campaigner, Max Schrems, alleging violations of GDPR as it pertains to the opt-in/opt-out clauses.

Failing to adhere to the GDPR has steep penalties of up to €20 million, or 4% of global annual turnover, whichever is higher.

V. COMPARISON OF INFORMATION TECHNOLOGY ACT, 2000 AND GDPR

This section deals with similarities and differences between key features of the GDPR and the IT Act. The following table presents key highlights of the similarities and differences described below:

PRINCIPLE	SIMILARITY	DIFFERENCES
OBJECTIVE	Used for Data transfer for electronic commerce.	GDPR specifically provides protection to natural persons and their rights and freedom upon data processing, which is not the case in the IT Act.
HOW PROCESSING AND COLLECTION OF DATA HAPPENS?	⇒ Collection of data should be for lawful purpose. ⇒ Collection should be necessary for the purpose specified.	The principles given in GDPR apply in relation to data processing. While the principles under IT Act apply to collection of information and use only. It does not mention processing. Principles listed in the GDPR but not mentioned in IT Act are data integrity, protection from unlawful processing,

		accountability, fairness and transparency.
LAWFULNESS OF PROCESSING	Consent of provider of information or the data subject is required for the purpose of collection of information and for processing under IT Rules and GDPR respectively.	Unlike the GDPR, the IT Act does not have a provision that specifically deals with "lawfulness" of processing. GDPR has five additional conditions required for processing and also give member states certain powers to introduce specific requirements for data processing. Such condition is not required according to IT Act.
CONSENT	Under both the laws: Consent before data collection is required. The provider has the power to take back his consent.	Unlike GDPR, the IT Act does not: ⇒ Define consent ⇒ List special conditions for child's consent ⇒ Require demonstration of consent by the data controller.

SENSITIVE PERSONAL DATA	Both laws include biometric data, health records and sexual orientation in the list of sensitive data.	GDPR and IT Act both have additional categories of sensitive personal data that are not common to the two laws.
RIGHTS	Some rules of Section 43A of the IT Act includes: • Right to rectification • Right to be informed • Right to withdraw consent. are same as the rights under GDPR.	Unlike the GDPR, IT Act does not use the word "Right". IT Act doesn't include rights which are there in GDPR like Right of access, right to restrict processing, right to data portability, right to object, right to erasure, right in relation to automated decision making and profiling. The Rights are described in brief in GDPR on contrary IT doesn't have such description of Rights.
SECURITY AND ACCOUNTABILITY	Common data protection security practices include adoption of internal policies, security audit, adherence to voluntary code of conduct and certification mechanism.	GDPR consists of additional and elaborate measures for security of data processing. These include appointing a Data Security Officer, conducting privacy impact assessment, maintenance of records of processing.

Compensation and Liability

The following table presents key highlights of the similarities and differences in respect of compensation and liability in the event of breach of such laws.

PRINCIPLE	SIMILARITY	DIFFERENCES
COMPENSATION FOR DAMAGES	Both laws provide compensation for the damages arising due to infringement. Both have relief from liability under certain conditions.	IT Act don't have compensation as a "Right" unlike GDPR.
PUNISHMENT IN CASE OF DISCLOUSER OF INFORMATION	Both have provision for fine in case of any breach.	Civil liability imposed in case of GDPR Criminal liability imposed in case of IT Act.

VI. CONCLUSION

The lack of a comprehensive legislation pertaining to privacy and data protection has been a matter of concern in India. This concern has been particularly expressed by foreign companies that are doing business in India and are transmitting confidential data into the country.

Even though the data protection laws are not specifically laid down in any statute as yet, the Indian industry as well as the have begun the process of sensitising the Government and the masses regarding the importance of privacy. Further, with regulators like the Reserve Bank of India providing for strict privacy norms in certain areas, it seems that India is taking a huge step towards privacy norms. It is being felt by all concerned that a dedicated data protection law would give further impetus to not only the outsourcing industry but to the Foreign Direct Investment Policy at large.

Bibliography

1. Information Technology Act, 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
2. White Paper on Data Protection Framework for India: [http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited]. (Accessed 25 Sept., 2019).
3. Regulation of the European Parliament and the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC (General Data Protection Regulation). EU official journal of 04.05.2016, L119, page 1.
4. Case **Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., 2017 (10) SCALE 1**, (2017) 10 SCC 1. An online copy of the judgment is available at https://indiankanoon.org/doc/91938676 (Accessed on 24 Sept., 2019),
5. Aadhaar Act available at https://uidai.gov.in/images/the_aadhaar_act_2016.pdf
6. TRAI, Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector, 2018, Telecom Regulatory Authority of India (Accessed on 24 Sept., 2019), https://www.trai.gov.in/sites/default/files/PRNo7816072018.pdf
7. Will a GDPR-Style Data Protection Law Work For India? By Anirudh Burman, May 15, 2019 available at https://carnegieindia.org/2019/05/15/will-gdpr-style-data-protection-law-work-for-india-pub-79113 (Accessed on 24 Sept., 2019)