PERSONAL DATA PROTECTION BILL, 2019: BALANCE BETWEEN SECTORAL AND GENERAL DATA PROTECTION FRAMEWORK

Research · May 2020

CITATIONS
0

READS
6

1 author:

Swikar Sankrit
Alliance University
8 PUBLICATIONS **0** CITATIONS

SEE PROFILE

PERSONAL DATA PROTECTION BILL, 2019: BALANCE BETWEEN SECTORAL AND GENERAL DATA PROTECTION FRAMEWORK

Swikar Sankrit[1]

[1] 5th year B.B.A. LL.B. student, Alliance School of Law, Alliance University, Bangalore, Karnataka

ABSTRACT

As the economies progress towards digitalization, data has become a valuable asset. Entities have been collecting personal data from their customers which has also led to misuse of user's data affecting their privacy. Right to privacy has been recently declared as a fundamental right in the case of *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.* and directed the government to prepare a personal data protection framework to protect the personal data of the citizens. Currently, personal data is protected under the Information Technology Act, 2000 and few other laws. Personal Data Protection Bill, 2019 has been presented in Lok Sabha in December 2019 which is currently being analysed by a Joint Parliamentary Committee. This Bill follows a comprehensive data protection approach which would apply equally to every entity, be it a big entity or a small entity. This Bill seems to affect small and medium sized business, innovations and emerging technologies. It is important to notice that small and medium sized businesses, innovations and emerging technologies are playing an important role in the growth and development of Indian economy, along with employment generation. US follows sectoral approach to data protection and have industry specific laws, whereas EU came up with GDPR which is a comprehensive data protection framework that regulates all the industries. This paper evaluates the objectives of Personal Data Protection Bill, 2019 to analyse whether India has followed GDPR as a model for data protection law, and how the Bill would affect the small businesses and emerging technologies, and would conclude if India needs to follow sector specific data protection law or a general data protection law.

Keywords: Personal Data, Privacy, Sectoral Approach, Comprehensive Approach, Personal Data Protection Bill, 2019

TABLE OF CONTENTS

CONTENTS **PAGE NO.**

1. Introduction

The right to privacy is a fundamental and natural right which is intrinsic to any individual. Although Indian Constitution doesn't expressly mention the right to privacy, the Supreme Court in the case of *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors*[2] held that Indian Constitution treats the right to privacy as a fundamental right and that privacy is enshrined in Article 21 of the Constitution under the right to 'life and personal liberty'. As of now, there is no data protection law in India that could compete with Europe's or US data protection framework. Currently, Information Technology Act, 2000 provides punishment for fraudulent and dishonest use of personal data. EU's data protection framework puts forth a general privacy law that is applicable to all the industries and the sectors that deal with the data relating to the citizens of European Union whereas US regulates privacy with a sectoral approach, with laws that are directed only to specific industries. The nine-judge bench of Supreme Court in the Justice K.S. Puttaswamy judgement directed the Indian government to enact an effective data protection law. Minister of Electronics and Information Technology Mr. Ravishankar Prasad tabled the Personal Data Protection Bill 2019 in Indian Parliament on 11 December 2019 and is currently being analysed by a Joint Parliamentary Committee.

Considering the Indian economy and government's USD 5 trillion target, it seems that upcoming data protection regime might hinder the target as such general data protection will increase compliance costs and challenges for service sectors, especially sectors like banking[3], IT, advertisement, customer care, among others. India is the sixth largest economy in the world, and this has been possible because of the high growth in IT industry which raked in more than USD 100 Billion[4] in export of IT software and services during the financial year 2017-18. The Personal Data Protection Bill 2019 would require companies to relook into the entire lifecycle of data starting from its generation, collection, storage and deletion, and would require the

[2] SC, W.P. (Civil) No. 494 of 2012 <https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf> accessed 10 February 2020

[3] Deepti Susan Thomas, 'GDPR and Its Impact on Indian Firms' *Deccan Herald* (28 October 2018) <https://www.deccanherald.com/business/economy-business/gdpr-and-its-impact-indian-700371.html> accessed 11 February 2020

[4] S. Sundararajan, 'How GDPR guidelines impact the Indian IT Industry' The News Minute (21 July 2018) <https://www.thenewsminute.com/article/how-gdpr-guidelines-impact-indian-it-industry-85174> accessed 11 February 2020

companies to revamp their existing business models. So, it becomes important to understand the objectives of the Personal Data Protection Bill, 2019 and if Indian economy is ready for such a general data protection law.

Chapter I of the paper deals with the existing data protection laws in India and objectives of the Personal Data Protection Law, 2019 through highlighting the main concepts of the Bill. Chapter II of the paper introduces the sectoral and comprehensive model of data protection law, and briefs about the data protection laws in US and EU, specifically GDPR. Chapter III of the paper analyses the role of innovations and emerging technologies, and how it has been impacted by GDPR, and how Personal Data Protection Bill, 2019 may affect the similar businesses in a developing country like India.

2. Data Protection Law in India

At present, India doesn't have a general data protection law, and has been governing personal data under sector specific laws like Information Technology Act, 2000 and Credit Information Companies (Regulation) Act, 2005. India is a party to Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which recognizes the right to privacy. Recently, India has tabled Personal Data Protection Bill, 2019 which seeks to regulate personal data in the hands of companies.

As the digital innovation continues to accelerate in India, it is very important to note that this disruption would be based on data, which further imposes a liability on government to protect the data of its citizens. The Supreme Court in the case of *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors*[5]recognised the right to privacy as a fundamental right under Article 21[6] of the Constitution of India which directed the government to enact suitable data protection law. Puttaswamy judgement articulates[7] the right to privacy as the right to bodily and mental integrity, the right to informational self-determination and right to decisional autonomy.

[5]*Ibid 1.*

[6] Protection of life and personal liberty No person shall be deprived of his life or personal liberty except according to procedure established by law.

[7] Gautam Bhatia. 'The Supreme Court's Right to Privacy Judgement', Vol. LII No. 44 November 4, 2017 Economic & Political Weekly, accessed 12 February 2020

Puttaswamy judgement also recognized the informational privacy as a part[8] of right to privacy and held that every individual is entitled to exercise his right to control the commercial use of his identity, information and personal information and that every individual should have the exclusive right to commercially exploit their identity, personal information and to control such information that is available on the internet.

2.1 Existing Laws

There are few sector specific legislations in India that deals with data protection, but not in as depth as the new proposed Bill. Information Technology Act, 2000 provides for safeguards against data breach from computer systems. However, S. 43A of the Act provides for the compensation for failure to protect data by body corporates. It further states that body corporate possessing, dealing or handling any sensitive personal data in a computer source controlled by them, is negligent in maintaining reasonable practice causing wrongful loss would be liable to pay damages to affected persons by way of compensation.[9]

S. 66C of the Act deals with punishment for identity theft and states that anyone fraudulently or dishonestly make use of the electronic signature, password or any unique identification of any person are to be punished with imprisonment of up to 3 years and with fine of up to Rs. 1,00, 000.

Further, S. 72A of the Act states that anyone who has access to personal information of any person, discloses it without the consent of that person to cause wrongful loss shall be punished with imprisonment of up to 3 years, or fine of up to Rs. 5,00,000, or both. Personal information[10] and sensitive personal data[11] has been defined in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Rule 4 of the IT Rules, 2011 requires body corporate and any person possessing, storing or handling data of information provider to publish privacy policy on their website

[8] *Ibid 6.*

[9] S. 43A, Information Technology Act, 2000

[10] Rule 2(i), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

[11] Rule 3, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011: password, financial information, physical, mental or physiological condition, sexual orientation, biometric information and medical records.

mentioning the type of personal data being collected, purpose of its collection and reasonable security practices being followed to prevent misuse of data.

S. 19 of the Credit Information Companies (Regulation) Act, 2005 requires credit company and credit institution possessing credit information to ensure that data maintained by them is complete, accurate and protected against any loss, unauthorised access and disclosure. Further, Chapter VI of the Credit Information Companies Regulations, 2006 provides for the privacy principles to be followed by credit information companies and credit institutions. These principles include obligation of companies, nature of data collection and also states that companies should retain collected data for a minimum period of 7[12] years.

Last but not the least, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. This Act requires concerned authorities to ensure[13] the security of identity information and authentication records of individuals. It also states that customer personal information collected by anyone for the purpose of authentication should be kept confidential[14] and used for the purposes specified and agreed with the customer.

2.2 Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019 was introduced on 11th December 2019 by Minister of Electronics and Information Technology Mr. Ravi Shankar Prasad in Lok Sabha. The Bill seeks to provide[15] for the protection of privacy of individuals relating to their personal data. This Bill follows the study of Justice B N Srikrishna Committee which was constituted to study the issues related to the data protection.

This Bill governs the processing[16] of personal data by state, any citizen of India, companies incorporated in India and foreign companies dealing with personal data of individuals in India and restricts the processing of personal data except for specific, clear and lawful purpose[17]. It

[12] Principle 7, Chapter VII, Credit Information Companies Regulations, 2006

[13] S. 28, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

[14] S. 29, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

[15] Personal Data Protection Bill, 2019 (373 of 2019)

[16] S. 2(A), Personal Data Protection Bill, 2019

[17] S. 4, Personal Data Protection Bill, 2019

also limits the processing for the purpose consented[18] to by the user in a fair, reasonable manner that ensures the privacy of the user. The Bill further provides for the collection and use of personal information, rights[19] of data principal[20] and obligations[21] of data fiduciary[22]. A data principal has the right to restrict[23] the continuing disclosure of his personal data, to obtain a copy of his personal data available with the data fiduciary, to get his personal data corrected, updated and erased. Data fiduciaries are required to implement privacy by design, comply with transparency requirements and create security safeguards to prevent misuse of data. They have additional obligations to appoint[24] data protection officers and to create grievance redressal mechanism. The Bill also proposes to establish Data Protection Authority of India to enforce data protection law. It would include every enterprise like IT companies, e-commerce giants, banks, hotels, restaurants, web aggregators which uses automated means to collect data.

The Bill mainly focuses on the processing of data on the basis[25] of free, informed, clear and specific consent by data principal and includes provisions that enables such consent to be withdrawn by the data principal. Any violation of these provisions would result in huge penalties[26]. This Bill also defines sensitive[27] personal data and requires explicit[28] consent for processing of such data. This Bill also requires the data fiduciary to provide a notice[29] to the data principal containing adequate information about the nature and purpose of data being collected, rights and obligations of data principal and data fiduciaries. This Bill also restricts data fiduciaries to not retain data beyond the duration necessary for processing and also requires them to delete the personal data after processing.

---

[18] S. 5, Personal Data Protection Bill, 2019

[19] Chapter V, Personal Data Protection Bill, 2019

[20] S. 3(14), Personal Data Protection Bill, 2019: Any natural person to whom personal data belongs.

[21] Chapter II, Personal Data Protection Bill, 2019

[22] S. 3(13), Personal Data Protection Bill, 2019: Any person/state/company determining the purpose and means of processing of personal data.

[23] S. 20, Personal Data Protection Bill, 2019: Right to be Forgotten.

[24] S. 30, Personal Data Protection Bill, 2019

[25] S. 11(2), Personal Data Protection Bill, 2019

[26] S. 57, Personal Data Protection Bill, 2019

[27] S. 3(36), Personal Data Protection Bill, 2019: includes financial data, health data, sex life, sexual orientation, biometric data, genetic data, religious or political belief.

[28] S. 11(3), Personal Data Protection Bill, 2019

[29] S. 7, Personal Data Protection Bill, 2019

Now, there is a provision in the Bill that allows central government to exempt[30] any agency of the government from the application of this law. Retired Judge B.N. Srikrishna, who chaired the committee that drafted the Personal Data Protection Bill, 2019 criticized the final version of Bill as he reasoned that government can access any personal data on the grounds of sovereignty, public order or security of the state which could limit the effectiveness of this new regime.

However, there is a provision that empowers the Data Protection Authority to create a sandbox[31] for the purpose of encouraging innovation in machine learning, artificial intelligence and emerging technologies in public interest, and entities involved in these business can apply for certain relaxations from application of some obligations under the law for maximum duration of 36 months. But there are few uncertainties as to the scope of definition of emerging technologies and what could be constituted within the scope of public purpose.

Further, this Bill requires data fiduciaries to store certain data in country. The Bill also imposes restriction on transfer of personal data outside India. The new data protection law would allow sensitive[32] personal data to be transferred outside India only for the purpose of processing and if explicit consent has been expressed by the data principal for such transfer, and such sensitive data shall be continued to store in India.

The Bill requires the critical personal data[33] to be processed only in India. There is no concrete definition of critical personal data in the Bill and which data would be considered as critical would be notified by the central government. Section 25 of the Bill requires data fiduciary to inform the Authority about the breach of any processed personal data that can harm data principal. The Bill also includes the concept of significant [34]data fiduciary which shall be notified by Authority on the basis of turnover, volume and sensitivity of data processed by data fiduciary. Significant data fiduciaries are required to undertake[35] a data protection impact assessment before commencement of data processing in case the processing involves new

[30] S. 35, Personal Data Protection Bill, 2019

[31] S. 40, Personal Data Protection Bill, 2019

[32] *Ibid 24*.

[33] S. 33, Personal Data Protection Bill, 2019

[34] S. 26(1), Personal Data Protection Bill, 2019

[35] S. 27(1), Personal Data Protection Bill, 2019

technologies or use of sensitive personal data which could pose a risk of significant harm to data principals.

Once enacted, this Bill would replace[36] the provisions related to personal data in Information Technology Act, 2000 and will prevail and have an overriding effect[37] over any law inconsistent with the provisions of this Bill.

3. Sectoral Data Protection Law v. General Data Protection Law

As the economies throughout the world progress towards the digital economy, data has become the most valuable asset. Protecting data and privacy rights have become a challenge for lawmakers. However, countries have come with their own data protection laws to ensure protection of personal data and privacy rights. There are different models that governments can employ for data protection. The two major methods of protection are comprehensive and sectoral laws.

Comprehensive laws are used by creating[38] a general law that governs the collection, use and processing of personal data or information by both public and private sector whereas sectorial laws are created through enacting separate laws for each industry, instead of having a general data protection law. European Union followed the comprehensive model for data protection and brought General Data Protection Regulation in 2016, which came into force in 2018. United States of America follows the sectoral legislation to protect the personal data of their citizens. The Health Insurance Portability and Accountability Act[39], 1996 is one of the sectoral laws that regulates the use and disclosure of protected health information by entities like health insurers and medical service providers. The Gramm–Leach–Bliley Act[40], 1999 governs the financial institutions with respect to collection, disclosure and protection of nonpublic personal information of consumers. The Fair Credit Reporting Act, 1970 was the first data protection

[36] S. 98, Personal Data Protection Bill, 2019

[37] S. 96, Personal Data Protection Bill, 2019

[38] Rebecca L. Woodard, 'Is Your Medical Information Safe? A Comparison of Comprehensive and Sectoral Privacy and Security Laws' (2004) Vol. 15(1) Ind. Int'l & Comp. L. Rev., pp. 147-182 <https://mckinneylaw.iu.edu/iiclr/pdf /vol15p147.pdf> accessed 10 February 2020

[39] Shawn Marie Boyne, 'Data Protection in the United States' (2018) Vol. 66(1) The American Journal of Comparative Law, pp. 299–343 <https://doi.org/10.1093/ajcl/avy016> accessed 10 February 2020

[40] *Ibid*.

law in US which was enacted[41] to enhance the accuracy, fairness and privacy of credit information of consumers. It regulates the collection, dissemination and use of consumer information including consumer credit information. Personal data in India, until the Personal Data Protection Bill, 2019 comes into force, is being regulated by sectoral laws.

Recently, California became the first state of the US to enact a general data protection law for consumers, i.e., California Consumer Privacy Act, 2018 which came into force on 3rd January 2018. This Act applies to any for-profit business that collects personal information of residents[42] of California and has annual gross revenue of more than $25 million[43] or buys, receives or sells the personal information of more than 50,000 consumers or derives more than 50% of the annual revenue from the sale of consumers' data. The Act provides the consumers with the rights[44] to know what personal information is being collected and to whom their data is being sold or disclosed, to deny the sale of their personal information, to access their personal information and to request the business to delete the collected personal information. The Act defines personal information as information that relates[45] to real name, postal address, unique identity number, IP address, email address, driving license number, social security number, passport number, or any similar identifier.

European Union enacted General Data Protection Regulation in May 2018 which governs[46] the protection of personal data of natural persons (EU citizens) and their rights and freedoms with regard to the processing of personal data. GDPR lays principles[47] for processing of personal data which requires the data to be processed in fair, transparent and lawful manner. Personal data under GDPR includes information[48] such as name, location data, online or social and cultural identifiers, economic information, physical, genetical or mental identifiers. It states that processing shall be lawful[49] if the user has consented to the processing of his data and for

[41] *Ibid*.

[42] S. 1798.140(g), California Consumer Privacy Act, 2018

[43] S. 1798.140(c), California Consumer Privacy Act, 2018

[44] S. 1798.110, California Consumer Privacy Act, 2018

[45] S. 1798.140(o), California Consumer Privacy Act, 2018

[46] Art. 1, General Data Protection Regulation

[47] Art. 5, General Data Protection Regulation

[48] Art. 4, General Data Protection Regulation

[49] Art. 6, General Data Protection Regulation

the legitimate purposes. Chapter 3 of the Regulation provides users the right to access[50] of personal data being processed, right to rectification[51] of inaccurate data, right to erasure[52] of personal data by the controller, right to objection[53] of personal data, right to data portability[54] from one data controller to another, right to not be subject of a decision based on automated processing except user's explicit consent[55]. The law requires the companies to have a clear privacy policy[56] stating the nature and purpose of data collection and rights of the user.

Data controllers are required to implement measures for data protection by design and default. It is the responsibility of the processor that the data controller[57] shall notify the data breach to the supervisory authority. It also requires that the controller shall carry out data protection assessment[58] if processing involves use of new technologies which could obstruct the rights and freedoms of natural persons. These regulations don't apply to processing of personal data by authorities for the purpose of investigation or prevention of criminal offences and public security[59] and non-compliance of GDPR attracts heavy penalties.

If both the GDPR and Personal Data Protection Bill, 2019 is compared as evaluated in Chapter 2.2 and Chapter 4, it could be said that Personal Data Protection Bill, 2019 stems out from the principals laid down in GDPR.

4. Indian Economy, Emerging Technologies and Data Protection Laws

Due to rapid change in technology, business have transformed the way they used to operate. In won't be wrong to say that finally world has entered in the first fully digital generation. This has led to the data becoming the most valuable asset in the world. Entities have been collecting

[50] Art. 15, General Data Protection Regulation

[51] Art. 16, General Data Protection Regulation

[52] Art. 17, General Data Protection Regulation

[53] Art. 21, General Data Protection Regulation

[54] Art. 20, General Data Protection Regulation

[55] Art. 22, General Data Protection Regulation

[56] Art. 13, General Data Protection Regulation

[57] Art. 4(7), General Data Protection Regulation: natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[58] Art. 35, General Data Protection Regulation

[59] Art. 2(2), General Data Protection Regulation

data and has been misusing for so long which led EU to enact GDPR. Similarly, India also came up with the GDPR like law that is about to be passed and enacted by the parliament.

It should be noted that micro, small and medium enterprises (MSMEs) are the backbone of the developing countries. India is also a developing country that MSMEs contributes significantly to the Indian economy in terms of Gross Domestic Product (GDP), exports, rural industrialization and employment generation. Currently, there are 6.33 crores MSMEs in India and employs more than 11[60] crore people in the sector. MSMEs share in Indian economy amounted to 28.9[61]% of total GDP in 2016-17 and share in total export from India was 48.1[62]% and generated employment of 5.87[63] lakhs in the in 2018-19. Personal Data Protection Bill, 2019 neither exempts MSMEs nor provides a threshold for availing exemption from the law. Now, if the proposed data protection Bill regulates the MSMEs, it would incur high costs in complying with provisions of data protection law, which could disrupt the sector, leading to loss of employment and would also hamper the economic growth of the country. An article by CUTS International Washington DC Center suggests that the bill may have an adverse impact[64] on MSMEs and startups.

The GDPR that rolled out in EU in 2018 negatively[65] affected[66] the EU economy and business, especially startups, drained resources of both companies and regulators and also reduced the competition. As per evidence, within one year of GDP, the investment in EU tech firms decreased by $14.1 million per month per EU member state. The major reason behind the

---

[60] Government of India, Annual Report 2018-19, Ministry of Micro, Small and Medium Enterprises (2019) <https://msme.gov.in/sites/default/files/Annualrprt.pdf> accessed 13 February 2020

[61] *Ibid*.

[62] Government of India, 'MSME Sector Contributes Significantly to Indian Economy' Press Information Bureau (22 July 2019) <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579757> accessed 15 February 2020

[63] *Ibid*.

[64] 'Personal Data Protection (PDP) Bill, 2019: Issues and Debate' (CUTS International Washington DC Center, 13 December 2019) <http://www.cuts-wdc.org/pdf/pdp-bill-2019-issues-and-debate.pdf> accessed 17 February 2020

[65] Eline Chivot and Daniel Castro, Center for Data Innovation, What the Evidence Shows About the Impact of the GDPR After One Year (2019) < http://www2.datainnovation.org/2019-gdpr-one-year.pdf> accessed 14 February 2020

[66] Council of European Union, Council Position and Findings on the Application of the General Data Protection Regulation (2019) <https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf> accessed 15 February 2020

negative impact is complexity of the GDPR that is very difficult to implement, even though Fortune 500 companies spent an estimated 7[67] billion euros in compliance costs for GDPR, the same isn't possible by small entities. The compliance costs are too high that small firms are moving away from EU market, which is the sole reason for reduced competition. Since, the Indian Data Protection Bill follows the provisions and principals of GDPR, it will most likely affect the MSMEs and startups in India too, which will further hurt the Indian economy and its goal to achieve $5 trillion economy. Reports also reveal that if India follows data localization measures, it would experience significant GDP loss[68] and reduction of domestic investment in India.

Apart from MSMEs, GDPR impacted even the emerging technologies as it restricts the entities to use personal data in the algorithmic economy. However, Indian Data Protection Bill has introduced the concept of sandbox which would encourage innovation in machine learning, artificial intelligence and emerging technologies and provide certain relaxations but there are few gaps in the law as it doesn't clearly define the scope of emerging technologies. As reported above, Fortune 500 companies spent more than 7 billion euros for complying with GDPR which suggests that these big tech firms don't require such exemption in India, rather such exemption should be given only to small startups. If similar incentives are given to all the entities, this would negatively affect the smaller entities and would reduce the competition in the market and will discourage the innovation in the country.

A study by European Centre for International Political Economy suggests that restrictive data laws have an adverse effect[69] on productivity of entities that uses data in producing goods and services. Further, one more study that evaluated the impact[70] of EU data protection framework on small and medium enterprises (SMEs) found that compliance to GDPR would incur huge

---

[67] *Ibid*.

[68] Anirudh Burman, 'Will a GDPR-Style Data Protection Law Work for India?' (Carnegie India, 15 May 2019) <https://carnegieendowment.org/files/4-17-19_Burman_India_GDPR.pdf> accessed 10 February 2020

[69] Martina Francesca Ferracane, Janez Kren, and Eric Marel, Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries? (European Center for International Political Economy DTE Working Paper, 2018) <https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Impact-the-Productivity-Performance-of-Firms-and-Industries-final.pdf> accessed 16 February 2020

[70] L. Christensen, The Impact of the Data Protection Regulation in the E.U. (Working Paper, 2013) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.138 &rep=rep1&type=pdf> accessed 17 February 2020

costs and would require entities to redesign their system and procedures for data protection which would negatively impact (especially job opportunities) the SMEs in EU. Thus, it can be inferred that GDPR like data protection law in India would cause significant loss to MSMEs and data driven startups. India being a developing country relies heavily on MSMEs for rural industrialization and India can't afford to demotivate these entities.

5. Conclusion

The specific model that the India chose to adopt for protection of personal data is expected to negatively affect the Indian economy. It would cause increased compliance costs for MSMEs and startups which would stifle innovation, economic growth and could also cause loss of employment. As discussed in Chapter III, India has blindly followed the GDPR model to govern the protection of personal data without undergoing the impact assessment of having such a law. It is better to have a sector specific data protection laws in India than having such a comprehensive law because it would only hinder the economic growth and cause negative consequences but if the government stills want to continue with such a law, it is important that clear classification be made in the law to exclude entities that could be negatively affected. The Bill should have included a threshold limit like in The California Consumer Privacy Act, 2018 to exclude smaller firms from the application of law. If clear classification is not done, the law would cause disruption of startups, innovation and have a negative impact on competition.

Currently, Bill is being analyzed by a Joint Parliamentary Committee and it is the time now that the committee should weigh the economic benefits of the proposed Bill. It is also important for the committee to consider the actual harms caused by the users or consumers, and then specifically draft the law to prevent such harms. The committee should consider the measures taken by the government to promote SMSEs and innovation, and then tailor the Bill accordingly to minimize the effect. The clear classification within the Bill could be the best way to minimize the effect, otherwise it is better that India should continue with the existing sectoral data protection laws and amend them to include the important provisions of the Bill.

Bibliography

Primary Sources:

Legislations

The Information Technology Act 2000 (21 of 2000)

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

The Credit Information Companies (Regulation) Act, 2005 (30 of 2005)

Credit Information Companies Regulations, 2006

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016)

The Fair Credit Reporting Act 1970

The Health Insurance Portability and Accountability Act 1996

The Gramm–Leach–Bliley Act 1999

The California Consumer Privacy Act 2018

Case Laws

Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors [WP (Civil) 494 of 2012] SC

Secondary Sources:

Regulations

The General Data Protection Regulation 2016/679

Bills

The Personal Data Protection Bill 2019 (373 of 2019)

Reports

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna Ministry of Electronics and Information Technology, Government of India, A *Free and Fair*

Digital Economy Protecting Privacy, Empowering Indians (2018) <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf > accessed 12 February 2020

Government of India, *Annual Report 2018-19, Ministry of Micro, Small and Medium Enterprises* (2019) <https://msme.gov.in/sites/default/files/Annualrprt.pdf> accessed 13 February 2020

Eline Chivot and Daniel Castro, Center for Data Innovation, *What the Evidence Shows About the Impact of the GDPR After One Year* (2019) < http://www2.datainnovation.org/2019-gdpr-one-year.pdf> accessed 14 February 2020

Council of European Union*, Council Position and Findings on the Application of the General Data Protection Regulation* (2019) <https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf> accessed 15 February 2020

Martina Francesca Ferracane, Janez Kren, and Eric Marel, *Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries? (*European Center for International Political Economy DTE Working Paper, 2018) <https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Impact-the-Productivity-Performance-of-Firms-and-Industries-final.pdf> accessed 16 February 2020

L. Christensen, *The Impact of the Data Protection Regulation in the E.U.* (Working Paper, 2013) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.138 &rep=rep1&type=pdf> accessed 17 February 2020

Research Papers

Franz-Stefan Gady, 'EU/U.S. Approaches to Data Privacy and the "Brussels Effect": A Comparative Analysis' (2014) IV Georgetown Journal of International Affairs. <https://www.jstor.org/stable/43773645?seq=1#metadata_info_tab_contents> accessed 10 February 2020

Rebecca L. Woodard, 'Is Your Medical Information Safe? A Comparison of Comprehensive and Sectoral Privacy and Security Laws' (2004) Vol. 15(1) Ind. Int'l & Comp. L. Rev., pp. 147-182 <https://mckinneylaw.iu.edu/iiclr/pdf /vol15p147.pdf> accessed 10 February 2020

Shawn Marie Boyne, 'Data Protection in the United States' (2018) Vol. 66(1) The American Journal of Comparative Law, pp. 299–343 <https://doi.org/10.1093/ajcl/avy016> accessed 10 February 2020

Emmanuel Pernot-Leplay, 'Emmanuel, China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?' (2020) Vol. 8(1) Penn State Journal of Law & International Affairs <https://ssrn.com/abstract=3542820> accessed 11 February 2020

Lothar Determann and Chetan Gupta, 'India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2019' (2018) Berkeley Journal of International Law <http://dx.doi.org/10.2139/ssrn.3244203> accessed 11 February 2020

Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla, 'The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India' (2019) The Centre for Internet and Society <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf> accessed 8 February 2020

Malavika Raghavan, Beni Chugh and Nishanth Kumar, 'Effective Enforcement of a Data Protection Regime: A Model for Risk-Based Supervision Using Responsive Regulatory Tools' (2019) Dvara Research <https://www.dvara.com/research/wp-content/uploads/2019/12/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> accessed 9 February 2020

'India Draft Personal Data Protection Bill, 2018 and EU General Data Protection Regulation: A Comparative View' (2019) Deloitte Risk Advisory <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-india-draft-personal-data-protection-Bill-noexp.pdf> accessed 10 February 2020

Gautam Bhatia. 'The Supreme Court's Right to Privacy Judgement', Vol. LII No. 44 (2017) Economic & Political Weekly, accessed 12 February 2020

Online Articles

'Supreme court holds that the right to privacy is a fundamental right guaranteed under the constitution of India' (*Nishith Desai Associates*, 7 September 2019) <http://www.nishithdesai.com/information/news-storage/news-details/article/supreme-court-holds-that-the-right-to-privacy-is-a-fundamental-right-guaranteed-under-the-constituti.html> accessed 10 February 2020

'State of Privacy India', (*Privacy International*, January 2019) <https://privacyinternational.org/state-privacy/1002/state-privacy-india> accessed 10 February 2020

Sushil Kambampati, 'What India's Data Protection Committee Can Learn from US, EU and China' *The Wire* (3 October 2017) <https://thewire.in/tech/what-indias-data-protection-committee-can-learn-from-us-eu-and-china> accessed 10 February 2020

Anirudh Burman, 'Will a GDPR-Style Data Protection Law Work for India?' (*Carnegie India*, 15 May 2019) <https://carnegieendowment.org/files/4-17-19_Burman_India_GDPR.pdf> accessed 10 February 2020

Andrada Coos, 'EU vs US: How Do Their Data Privacy Regulations Square Off?', (*Endpoint Protector*, 17 January 2018) <https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/> accessed 10 February 2020

Deepti Susan Thomas, 'GDPR and Its Impact on Indian Firms' *Deccan Herald* (28 October 2018) <https://www.deccanherald.com/business/economy-business/gdpr-and-its-impact-indian-700371.html> accessed 11 February 2020

S. Sundararajan, 'How GDPR guidelines impact the Indian IT Industry' *The News Minute* (21 July 2018) <https://www.thenewsminute.com/article/how-gdpr-guidelines-impact-indian-it-industry-85174> accessed 11 February 2020

Eline Chivot and Daniel Castro, 'The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy' (*Center for Data Innovation*, 13 May 2019) <https://www.datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/> accessed 12 February 2020

Government of India, 'MSME Sector Contributes Significantly to Indian Economy' *Press Information Bureau* (22 July 2019) <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579757> accessed 15 February 2020

'Personal Data Protection (PDP) Bill, 2019: Issues and Debate' (*CUTS International Washington DC Center,* 13 December 2019) <http://www.cuts-wdc.org/pdf/pdp-bill-2019-issues-and-debate.pdf> accessed 17 February 2020