Volume 11, July 2020 ISSN 2581-5504

"Understanding the Need for a Data Protection Regime in India"

Neha Joshi

INTRODUCTION

There is a significant rise in the availability and storage of personal information on online platforms leading to a rise in the analysis of data and ease of mining of personal information and necessity of public policy to manage such data to balance the benefits of collection of huge data and protection of privacy.[1] Information has become the nucleus and flows freely cross-border.[2] This is not just a shift in the paradigm of information technology but has also brought the concern of privacy to the fore. Transnational corporations are increasingly utilizing private and public international networks and have already distributed computing and data processing across the globe. The problem of privacy has thus become a complicated global issue.[3]

The United States of America was the first country to take up the issue of privacy as a public issue and for the longest period, it was a piece of legislation with the broadest applicability.[4] Thus was born the Privacy Act of 1974 for protecting the administrative records held by governing agencies. Thereafter, there have been several privacy codes, majorly in the European continent, which has carved out principles for protection of privacy used as a framework guideline in other jurisdictions.[5]

It has been over two years since the enforcement of the General Data Protection Regulation ("GDPR") by the European Union ("EU") and 67 out of 120 countries outside of Europe have largely adopted this framework.[6] There is a rise in corporations coming up with business models relying heavily upon processing of data received from private and public international networks. The Indian government on the other hand grapples with the issue of storage and protection of sensitive personal data of the citizens on a humungous scale. With this backdrop, this paper examines the pattern of data protection regime of a technologically dependent country like India which did not have a comprehensive data protection regime like the EU, until the introduction of the Personal Data Protection Bill, 2019 ("PDPB").

---

[1] Vrinda Bhandari & Renuka Sane, *Protecting Citizens from The State Post Puttaswamy: Analysing The Privacy Implications of the Justice Srikrishna Committee Report And The Data Protection Bill, 2018*, 14 SOCIO-LEGAL REVIEW 27, 144 (2018).

[2] COLIN J. BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE xvi (2006).

[3] *Id.* at xviii–xix.

[4] Lee A. Bygrave, *International Agreements to Protect Personal Data*, *in* GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION , 4 (2008).

[5] *Id.* at 9.

[6] JUSTICE B. N. SRIKRISHNA & COMMITTEE OF EXPERTS, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* 3 (2017), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited Oct 15, 2019).

Volume 11, July 2020 ISSN 2581-5504

This paper examines the data protection regime of India, comparing the GDPR and PDPB. Since the GDPR is freshly enacted, countries and corporations all over the world are still figuring out the manner of implementing the provisions, and hence it is too early to find out how the regulation has fared. The Indian Bill, on the other hand, is yet to be enacted and has the advantage of making improvements based on the criticisms received for the GDPR.

The present paper attempts to map out the trend of data protection laws in India and how it has been influenced by the prominent laws of the European continent. The first part of the paper deals with how Europe as a continent developed its data protection laws and continued to update it thereby dominating the world in data protection laws and setting the ideal threshold to follow. The second part of the paper deals with how India as a developing country developed its data protection regime. The final two parts of the paper specifically deal with the most impactful piece of law rolled out by the European Union i.e. the GDPR and whether it is the inspiration behind India's first comprehensive data protection law – PDPB.

DATA PROTECTION IN EUROPE

There was anxiety upon the advent of the use of Information Technology widely. It called for legal control and regulation-based control over the collection and usage of personal data. One by one, countries in Europe[7] introduced national legislation for data protection.[8]

At the start of 1980, Europe saw two important international instruments being introduced:

1. Organisation for Economic Co-operation and Development's (OECD) Guidelines of 1980 ("OECD Guidelines") governing the Protection of Privacy and Transborder flows of personal data, and

2. The Council of Europe's Convention for Protection of Individuals concerning the Automatic Processing of Personal Data of 1981.

OECD GUIDELINES

The guidelines have at their core a set of eight data principles to be applied for manual and electronic processing of personal data.[9] The eight principles are the following:

[7] Few instances being German State of Hesse in 1970, Sweden in 1973, West Germany in 1977 and France in 1978

[8] ANDREA MONTI & RAYMOND WACKS, PROTECTING PERSONAL INFORMATION: THE RIGHT TO PRIVACY RECONSIDERED 19 (2019).

[9] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, , ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (2013),

Volume 11, July 2020 ISSN 2581-5504

1. Collection limitation;
2. Data equality;
3. Purpose specification;
4. Use limitation;
5. Security safeguards;
6. Openness;
7. Individual participation; and
8. Accountability

The guidelines although not legally binding have been influential on the enactment and content of the data protection legislation in countries even outside of Europe, namely Japan, Australia, New Zealand, Canada and Hong Kong. Additionally, it has been a source of inspiration for the Asia-Pacific Economic Co-operation's Privacy Framework of 2004.[10]

EUROPEAN UNION DIRECTIVE

The European Parliament and the Council of Europe passed the EU Directive 95/46 on the 24th October 1995.[11] The intention of the Directive was to protect personal data and free movement of such data of individuals. After introducing the GDPR, 2018, the Directive has ceased to become enforceable however it is pertinent to understand the intention of the Directive to understand how the regime of data protection begun and is still developing.[12]

The Directive did not cover activities processing data which fell beyond the ambit of the EU. Member states of the EU were required to lay down exemptions from the central provisions

https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Nov 22, 2019).

[10] OECD Working Party, OECD Guidelines governing the protection of privacy and transborder flows of personal data 20 (1980), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last visited Jul 21, 2020).

[11] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, , OJ L 281 (1995), http://data.europa.eu/eli/dir/1995/46/oj/eng (last visited Aug 14, 2019).

[12] European Commission, *Communication from the Commission to the European Parliament and the Council*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0043 (last visited Nov 24, 2019).

of the Directive for data processing.[13] Moreover, it stated that law of one Member State of EU can be applied outside the state of EU in circumstances where there is a data controller appointed outside EU utilizing 'equipment' located inside the particular Member State to process personal data.[14] The Directive was unique and different from the other international data privacy instruments for providing basic information about the scope of data-processing operations to the data subjects.[15]

The basic rule in the Directive was that transfer of data is permitted outside the EU if the third country ensures an adequate level of protection.[16] However, a drawback of the Directive was that 'adequacy of protection' was not defined, and the criterion was implied to mean 'a less stringent standard than the criterion equivalent in the CoE Convention and OECD Guidelines'.[17] No other international code went this far to control the flow of personal data to an international state not offering the same level of protection as the level offered by the EU Directive.[18] This justification could have softened the potentially negative impact of Article 25(1) on data flows to countries outside the EU. For instance, in the early years, there was tension between the United State of America and the EU after adoption of this Directive. This cooled after the adoption of the 'Safe Harbour' Scheme which recognized that organizations were qualified to offer adequate protection for the processing of personal data according to their adherence to a basic set of principles inspired from the EU Directive.[19]

GENERAL DATA PROTECTION REGULATION ("GDPR")

In May 2018, the EU rolled out the GDPR harmonizing data protection and privacy requirements across the EU.[20] GDPR retained the basic principles of the EU Directive and that can be seen concerning the transfer of personal data to countries outside of Europe which is permitted only if the countries have been found to have an adequate level of data protection.[21] Following the enactment of the Regulation, the EU and Japan agreed with the free flow of personal data between the two economies once Japan could prove that they have

[13] Article 28 of the Directive included data processing done solely for the purpose of 'journalistic purposes or literary expressions insofar as is necessary to reconcile the right to privacy with the rules governing freedom of expression'. See, Article 28 DIRECTIVE 95/46/EC, *supra* note 11.
[14] Article 4(1)(c), *Id.*
[15] Article 10 and 11, *Id.*
[16] Article 25(1), *Id.*
[17] Bygrave, *supra* note 4 at 38.
[18] *Id.* at 37.
[19] *Id.* at 41.
[20] Razvan Viorescu, *2018 Reform of EU Data Protection Rules*, 4 EUROPEAN JOURNAL OF LAW AND PUBLIC ADMINISTRATION (2017).
[21] Article 45, DIRECTIVE 95/46/EC, *supra* note 11.

an adequate level of data protection.[22] However, GDPR has introduced some new provisions which are as follows:[23]

1. The definition of 'personal data' has included every kind of information that could identify individuals.
2. Concept of 'Data processors'[24] and 'Data controller'[25] has been introduced and they have been directed to demonstrate how they are complying with the principles in GDPR.
3. The definition of consent[26] indicates that consent should not only be prior consent but also free and informed and companies should be able to demonstrate how the consent was obtained so that the user can be allowed to withdraw their consent.
4. GDPR introduced the concept of data protection officer[27] who is required to be appointed where large scale data is being collected.
5. Data subjects can request and get access to their data and how it is being processed. The timeline for providing such access is one month from the date of request.
6. A very important and prominent introduction through the GDPR is the significant increase in exposure to penalties and the quantum of fines to be levied for breach in 'record-keeping, security, breach notification, etc.' A penalty of up to €10 million or 2% of the worldwide annual revenue of the prior financial year, whichever is higher is levied for infringement caused controllers and processors,[28] or by the certification body[29] or the monitoring body[30]. A penalty of up to €20 million or 4% of the worldwide annual revenue of the prior financial year, whichever is higher will be issued upon failure to abide by the basic principles of processing,[31] violation of the

[22] Apart from Japan, the EU has agreed to a similar arrangement with 13 other countries: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework). See, Soumyarendra Barik, *India to seek "adequacy" status with the GDPR after Data Protection bill is passed: report*, MEDIANAMA (2019), https://www.medianama.com/2019/07/223-india-to-seek-adequacy-status-with-the-gdpr-after-data-protection-bill-is-passed-report/ (last visited Nov 20, 2019).

[23] Bhumesh Verma & Soumya Shekhar, *The GDPR Giant and How to Tackle It: An Indian Perspective*, CORP COMM LEGAL 69 (2018).

[24] Article 4(7), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, AND REPEALING DIRECTIVE 95/46/EC, (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (last visited Jul 21, 2020).

[25] Article 4(8), *Id.*

[26] Article 4(11), *Id.*

[27] Article 37, *Id.*

[28] Articles 8, 11, 25-39, 42 and 43, *Id.*

[29] Articles 42 and 43, *Id.*

[30] Article 41 (4), *Id.*

[31] Articles 5, 6, 7, and 9, *Id.*

data subjects' rights,[32] violation of transfer of personal data to a recipient in a third country,[33] etc.

The EU model provides an all-inclusive data protection law for the processing of personal data. It possesses a broad data protection structure and protection from processing activities carried out in both the public and private sectors.[34]

DATA PROTECTION IN INDIA

Taking a cue from countries like Japan, if India wants to approach the EU for an adequacy status, it would have to install a data protection regime nationally first.[35] The Supreme Court of India noted in its judgment of 2017 that in India, damages for privacy violation were governed under the tort law.[36] So far, the Information Technology Act, 2000 is the most important legislation dealing with data privacy issues particularly sections 43 and 43A. There have been only a handful of judicial interpretation, however, none of the Supreme Court.[37]

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, comes close to resemblance with a data protection law.[38] But these rules have their share of deficiencies; no consumer so far has exercised these rights under it.[39]

The Government constituted a Committee of Experts chaired by Justice B. N. Srikrishna to review data protection norms in India and the Committee submitted its final report[40] along with the draft law of 'The Personal Data Protection Bill, 2018' ("The Bill"). The Bill regulates the processing of personal data of individuals[41] by government and private entities incorporated in India and outside India.

The Bill allows exemptions for certain kinds of data processing[42] just like in GDPR. A significant difference from GDPR in the Bill was the requirement of serving a copy of the

[32] Articles 12 to 22, *Id.*
[33] Articles 44 to 49, *Id.*
[34] There are certain exemptions from protection when the processing of data is for the purpose of national security, defence, public security, etc. See, Ministry of Electronics and Information Technology, *Data Protection in India* (2018), https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf.
[35] Barik, *supra* note 22.
[36] Justice K. S. Puttuswamy (Retd.) v. Union of India and Ors., , 10 SCC 1, 123 (2017).
[37] GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE & HUMAN RIGHTS PERSPECTIVES 413 (2014).
[38] *Id.* at 414.
[39] *Id.* at 413.
[40] JUSTICE B. N. SRIKRISHNA AND COMMITTEE OF EXPERTS, *supra* note 6.
[41] Termed as data principals in the Act
[42] Processing in the interest of national security, for legal proceedings, or for journalistic purposes

personal data stored within the territory of India more specifically the critical personal data.[43] Further, similar to the GDPR, the Bill provided for penalties levied on the data fiduciary for failure to comply with the following: 'Data processing obligations, requirements of cross-border data storage and transfer requirements, etc.[44]

While the Bill places this obligation on all data fiduciaries, it does not specify any principles or guidelines for what constitutes a 'fair and reasonable' manner of personal data processing. The absence of guiding principles could allow fairness and reasonability standards to vary across fiduciaries processing similar types of data; fiduciaries in the same industry may develop and follow different standards. Further, in the absence of any guidelines, it may be unreasonable to expect the fiduciary to demonstrate compliance.

Although the Bill is still a Draft and, the impact it would have, cannot be assessed as on date, however, the bill itself received certain comments to ensure a smooth functioning once enacted. Some of the criticisms raised are:[45]

1. Although non-consensual processing of data given to Government entities is considered to be too wide a power, the Bill still allows for non-consensual data processing.
2. 'Serving copy' and 'critical personal data' are not defined in the Act.
3. Why there is a need to store a copy of the data within the country is unclear.
4. Due to additional costs of setting up duplicate servers, the data fiduciaries may get discouraged from investing in the Indian market.
5. The additional costs incurred by the data fiduciary may be passed on to the consumers.
6. A provision of the Bill consists of notifying the user about the collection of data to get the user's consent. Now, this was present in the EU directive as well as the GDPR, but it leads to a 'consent fatigue'. This ought to be suitably revised.[46]

INFLUENCE OF THE GPDR ON THE BILL

We can easily draw a parallel between the two data protection laws – the GDPR from EU and the Bill of India – to see how data protection principles have travelled and influenced from

[43] Draft Personal Data Protection Bill, 2018, , PRS LEGISLATIVE RESEARCH , https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018 (last visited Jul 21, 2020).
[44] *Id.*
[45] *Id.*
[46] Rajesh Vellakkat, *Personal Data Protection Bill: Will it Disrupt our Data Ecosystem?*, THE FINANCIAL EXPRESS (2019), https://www.financialexpress.com/india-news/personal-data-protection-bill-will-it-disrupt-our-data-ecosystem/1647076/ (last visited Nov 24, 2019).

the GDPR into the Bill. We can further note as to how Bill has attempted to consider the drawbacks of the regulation.[47]

1. **With respect to the territorial scope,** two provisions ought to be brought to light herein:

    a. The anonymization standards between the GDPR and Bill may differ, so compliance with both legislations separately is mandatory for companies. This could be managed to align with one of the data protection legislations in order to make it easier for private institutions to expand their business and for users to seek reliefs in adjudication.

    b. Secondly, the definition of sensitive personal data and having a provision of critical personal data is an improvement of the Bill taking into consideration the limited definitions in the GDPR.

2. **With respect to notice and consent,** the GDPR gave a holistic definition on what constituted a valid consent and based on the same principle the Bill also defined consent. However, the bill went further to give more clarity on the legal consequences of withdrawing of consent.

3. **With respect to data processing principles,** the GDPR has powers to retain data for longer time for processing as opposed to the Bill which only allows longer retention only if it is mandated by law.

4. **With respect to security and compliance,** inspired from the OECD and GDPR, the Bill has also retained the principle of protecting privacy by way of incorporating in the design.

5. **With respect to grievance redressal and penalties,** the Bill has chosen to soften its stand as to penalty that will be imposed if there is any violation of the data fiduciary. The Bill has a lower amount of penalty as opposed to the GDPR by a huge difference. For grievance redressal, there is an appellate body provided in the Bill as opposed to the GDPR, which does not have any.

CONCLUSION

Upon perusing the legislations laid down by EU so far, it is evident that European Union are the trendsetters for the data protection regimes. It is obvious that the regulation will have an

[47] Ikigai Law, *Comparative analysis: General Data Protection Regulation, 2016 and the Personal Data Protection Bill, 2018* (2019), https://www.ikigailaw.com/comparative-analysis-general-data-protection-regulation-2016-and-the-personal-data-protection-bill-2018/ (last visited Nov 29, 2019).

Volume 11, July 2020 ISSN 2581-5504

influence on the member states' national laws, but the new GDPR has managed to influence, rather mandate, other non-EU members to sit back and take a look at their own data regime in order to come at par with the EU data protection regime.[48]

Before EU came up with the revolutionizing data protection regimes, the discussion with respect to privacy was always limited to the protection of human rights and little about criminal actions against minor violations here and there. Now the discussion has moved on to cross-cutting issues like terrorism, national society and enforcement of law.[49] Now, there are several companies whose existence and business is based on data and its processing.[50]

However, these companies just cannot keep focusing on being compliant with two different regimes. As stated herein above, the Bill is influenced by the GDPR but a close perusal of each provision shows how being compliant with one wouldn't translate to being compliant with the other. Those laws cannot be used inter-changeably. Both these regimes – EU and India – are favorable markets in the world. Having different regimes and forcing companies to be compliant with both may be imposing additional burdens on them. [51]

Having said that it also cannot be denied that any private entity which has already proceeded to undertake the GDPR compliance, like creating a data inventory, carrying out assessment of data processing, placing procedures to manage data breaches, and carrying out anonymization/pseudonymization of data will be in a better position to adapt their policies to the Bill or any other future laws that may be modeled on the GDPR.

[48] Bygrave, *supra* note 4 at 47.
[49] *Id.* at 48.
[50] Bhandari and Sane, *supra* note 1 at 144.
[51] Ikigai Law, *supra* note 47.