CARNEGIE INDIA

MAY 2019

Will a GDPR-Style Data Protection Law Work for India?

ANIRUDH BURMAN

The European Union's (EU's) General Data Protection Regulation (GDPR) took effect in May 2018, harmonizing data protection and privacy requirements across the EU.[1] Many other countries have either implemented data protection requirements or are in the process of considering them. In the United States, for example, Senator Elizabeth Warren has proposed a bill to expand criminal liability for the executives of companies that suffer data breaches.[2]

India, too, is taking steps to enact a data protection framework modeled along the lines of the GDPR. In July 2017, the government of India appointed a Committee of Experts on a Data Protection Framework for India, or Data Protection Committee (DPC), under the chairmanship of Justice B.N. Srikrishna, to study issues related to data protection in India.[3] Though the committee submitted its report—and proposed a comprehensive law on data protection—on July 27, 2018, it failed to weigh the economic costs and benefits of implementing a GDPR-style law in India.

Emerging economies—like India—that are considering such proposals need to carefully evaluate the direct and indirect costs of such laws vis-à-vis the benefits from a data protection framework. A survey of the existing literature that estimates these costs and benefits highlights the need for further research on data protection laws.

The proposed law, called the Personal Data Protection Bill (hereafter, the bill), incorporates many elements of the EU's GDPR.[4] These include requirements for notice and prior consent for the use of individual data, limitations on the purposes for which data can be processed by companies, and restrictions to ensure that only data necessary for providing a service to the individual in question is collected. In addition, it includes data localization requirements and the appointment of data protection officers within firms. If enacted, the bill will provide a comprehensive, cross-sectoral privacy and data protection framework 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. As a legislative proposal that will have a significant impact on critical sectors of India's economy, it is vital that the DPC's proposed bill be carefully and critically evaluated.

INDIA'S DRAFT DATA PROTECTION LAW

While the EU has recognized a right to the protection of personal data for a while now (under the Treaty on the Functioning of the European Union), India still does not have a cross-sectoral law on data protection. The Information Technology Act of 2000 primarily governs issues such as cyber crime and the liability of internet intermediaries, such as social media platforms, though it does possess some requirements regarding the protection of personal data.[5] For example, section 43A of the act provides compensation for damages caused by a failure to maintain reasonable security practices to protect sensitive personal data. Data protection and confidentiality requirements, however, are regulated only by a patchwork of sector-specific regulatory requirements.

In August 2017, the Indian Supreme Court declared the right to privacy to be a part of the fundamental right to life under Article 21 of the Indian Constitution.[6] It held informational privacy to be a subset of this right to privacy, and noted that privacy includes the right to protect individual identity. This essentially implied that the patchwork approach to privacy embodied in existing laws was insufficient, and that a more comprehensive approach to informational privacy would be required. The judgment noted that the Indian government had already constituted the DPC and, in effect, gave its own sanction to the committee's workings.[7] However, though the DPC evaluated different legal frameworks for protecting privacy in different countries, it chose to propose a bill modeled largely after the GDPR.

These similarities extend to several concepts and legal requirements, including:

- Data processing (the collection and analysis of personal data) and data principals (persons or entities that provide data that is then used by firms for data processing).[8]
- Notice and consent requirements for the processing of personal data.[9]
- Limitations on the processing of personal data, including minimization requirements—only collecting data that is necessary to provide the services the data processor has agreed to provide to the user.[10]
- Compliance requirements for data processors, such as incorporating privacy by design, and the appointment of data protection officers to conduct periodic data protection impact assessments and data audits.[11]
- Providing positive rights to users, such as the right to data portability (to migrate data from one service provider to another) and the right to be forgotten.[12]
- The requirement of data localization—critical personal data is to be stored on servers within India, and there are constraints on the transfer of other personal data outside India.[13]
- Regulation and supervision by a proposed Data Protection Authority.[14]

- Penalties, including the prohibition of processing, and financial consequences for noncompliance.[15]

The bill does, however, differ from the GDPR in some respects—the most significant being the provision of criminal penalties for harms arising from violations of the bill,[16] and the proposal to treat the relationship between a data processor and its consumer as a "fiduciary" relationship.[17]

Nevertheless, these provisions in the bill would increase data protection obligations significantly. The bill would enforce economy-wide changes to the data collection, storage, and management practices of Indian businesses, as well as foreign firms that provide services within India.[18] While the EU had a preexisting privacy framework (the 1995 Data Protection Directive),[19] the bill would be a novel data protection framework for India. The cost of compliance and data protection obligations would, therefore, be much higher for India. In addition, no systematic economic analysis of the proposed bill has been conducted yet to provide an accurate analysis of its overall impact within India.[20]

IMPACT ASSESSMENTS OF THE GDPR

In 2012, the European Commission released an impact assessment (EU IA) of the then-proposed GDPR,[21] which provided a holistic overview of the potential costs and benefits of the proposed regulation. The range of factors that it considered in its assessment, as well as the conclusions it drew, are relevant to India's proposed adoption of a GDPR-style law.

Firstly, the EU IA found that businesses and consumers operating within multiple jurisdictions of the EU faced significant costs. The EU IA notes that, in the pre-GDPR framework, a number of broadly formulated provisions gave member states considerable flexibility in implementing them. This led to varied treatment toward consent requirements, categories of "sensitive" data, and notifying host country authorities about data-processing activities.[22] Secondly, the EU IA highlighted the differences in data protection rights within EU member countries, the lack of an effective channel for redress, and "insufficient awareness and identification of privacy risks" as issues that undermined user confidence in the online environment.[23] Thirdly, the EU IA noted the existence of significant gaps and inconsistencies in matters of police and judicial cooperation within the EU. These issues, according to the EU IA, created the need for a more harmonized framework that would increase legal certainty, reduce fragmentation, and bring consistency to the enforcement of data protection laws.

The key motivations behind implementing the GDPR, therefore, were to ensure (a) a high level of data protection for individuals in the EU, (b) an equivalent level of data protection among all member states, and (c) the free flow of information within the EU.[24] In consequence, while the EU IA recognized that the implementation of the GDPR would entail significant compliance costs, it calculated that the implementation of the GDPR would be an overall benefit to the EU.[25]

The UK Ministry of Justice, however, disagreed with the EU IA in its own impact assessment (UK IA).[26] The UK IA calculated the costs of appointing data protection officers, undertaking the data protection impact assessments, and notifying the supervisory authority of data breaches, and found that the costs of implementing the GDPR in the UK would outweigh its benefits.[27]

The UK IA also found lower benefits from legal harmonization based on its own estimates, and argued that the proposed gains from harmonization across the EU were overstated due to the flexibility in implementation that the GDPR would provide to member countries.[28] The UK IA also points out that small businesses are less likely to benefit from harmonization compared to large multinational

corporations. It argued that SMEs in the UK, in particular, would face increased compliance costs due to the lack of in-house expertise in managing additional compliance burdens.[29]

The European Center for International Political Economy (ECIPE) also published a number of studies assessing the costs of the GDPR. One study, which focused on the external or cross-border implications of the GDPR, found that the EU IA did not examine the GDPR's consequences for trade and cross-border transactions.[30] The study noted that while the export of U.S. services to the EU would be negatively affected by the GDPR, the EU's export of services to the United States would be affected much more severely.[31] It goes on to add that the implementation of the right to be forgotten would worsen the negative effects of GDPR implementation.[32] The study also estimated a significant overall drop in the EU's GDP—between 0.8 to 1.3 percent if foreign businesses were required to establish businesses within the EU in order to handle EU citizens' data transfers.[33]

Another ECIPE study on the impact data localization requirements in the GDPR noted that,

> Manufacturing and exports sectors are also dependent on having access to a broad range of services at competitive prices—such as logistics, retail distribution, finance or professional services—which in turn are heavily dependent on secure, cost-efficient and realtime access to data across borders. . . . Thus, increased regulation leads firstly to domestic productivity losses for various sectors of the economy. Secondly, it creates an additional trade barrier against data processing and internet services, or any service . . . that depends on the use of data for delivery. Thirdly, as the competitiveness of the economy changes, investments (both domestic and foreign) will be affected.[34]

The study goes on to state that if other economies—such as India, Brazil, Indonesia, South Korea, or Vietnam—also impose similar economy-wide data localization measures, they could experience significant GDP losses. In India, for example, it estimates a loss of up to 0.8 percent of GDP should the country adopt a localization requirement. The study also estimates a reduction of up to 1.4 percent of domestic investments in India due to localization requirements.[35]

Another ECIPE study, "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?," argues that restrictive data policies have a significant negative impact on firm productivity in sectors that use data to a significant extent in producing goods and services.[36] It also finds that this impact is compounded if the firm is placed within a country that has stricter requirements regarding the use and transference of data.

Further, a study by L. Christensen and others found that compliance costs would have a significant negative impact on EU SMEs,[37] as GDPR compliance would require EU firms to completely redesign their systems and procedures for data protection. For many Indian SMEs, the lack of a preexisting data protection law would make this a de novo exercise, consequently compounding the costs. Compliance procedures—such as data protection impact assessments—would have to be incorporated into information technology management systems, along with the data protection officer's role within the functioning of business firms. The study goes on to note that the search for professionals with the appropriate labor skills related to data protection (for example, a data protection officer) is also expected to add "friction" to the EU's unemployment market by impacting a firm's job creation decisions:

> Finding appropriate candidates for a new job opening requires time. This is of course costly for firms. The presence of search costs in the labor market leads to a frictional level

> of unemployment. Any event that affects the expected surplus that a newly created job could deliver may impact on firms' job creation decisions. This is the channel through which regulation could affect job creation.[38]

This could reduce long-run sectoral employment within the EU by 0.3 percent,[39] and the number of companies themselves could reduce by 3 percent.[40]

Another set of literature points to tensions between emerging technologies and some of the requirements set out in the GDPR. One paper, for example, argues that the specific obligations of data processors are fundamentally incompatible with big data.[41] It states that big data aggregates and processes information about individual behavior in a variety of situational contexts, and the requirements of prior and informed consent, purpose limitation, and rights against automated processing "[undermine] the abilities to engage in Big Data in general."[42] Similar concerns have been laid out with regard to the use of blockchain and the anonymization and pseudonymization requirements in the GDPR.[43]

LESSONS FROM THE GDPR'S IMPACT ASSESSMENT REPORTS FOR INDIA

An analysis of the GDPR impact assessment literature raises several significant issues in adopting a GDPR-style law for India.

First, even if legislation like the GDPR or the proposed data protection bill is intended to protect fundamental rights, the specific mechanisms within such legislation should be evaluated carefully. For example, though the EU treats informational privacy as a fundamental right, it nevertheless published the EU IA estimating the potential costs and benefits of the proposed GDPR. This EU IA then formed a basis for the further study and critique of the proposed GDPR. The report of the DPC in India, however, did not discuss the potential economic impact of the proposed bill. A careful estimation of the costs and benefits of the specific obligations within the proposed bill is therefore imperative before further progress on the bill can be made.

Second, the EU IA argued that the *key economic* benefits of enacting the GDPR in the EU would result from the harmonization of privacy standards.[44] Considering that India does not suffer from the problems of a preexisting, fragmented regulatory framework in data protection, it is worth asking what economic benefits would accrue to India from the proposed bill. India's patchwork of central laws that currently affect privacy were enacted by the federal parliament and are therefore uniformly applicable across India. Therefore, if one were to consider the three main benefits of the GDPR for the EU (as per the EU IA) in relation to India, at least one of them does not have immediate relevance.

Enacting a law that protects personal data would be undoubtedly beneficial. It would provide certain safeguards against misuse and legal recourses against harm caused by this misuse. However, such a law should be specifically designed to be contextually relevant, without creating negative consequences for the economy as a whole. For example, if India does not stand to benefit from the harmonization of existing legal requirements, what are the other sources of benefit that would outweigh the costs of a GDPR-style law?

While the report of the DPC is based on an extensive survey of *legal frameworks* in use worldwide, it does not provide any estimation of the probable *economic* impact of the proposed bill. Therefore, answering this question on the basis of the DPC's report is difficult, since it does not provide any assessment of the actual harms currently being suffered by consumers in India and how the bill is specifically tailored to prevent or deter them.

The need to understand the impact of a cross-sectoral

privacy law on employment, job growth, and small businesses is much more important for an emerging economy like India. As per one independent source, job growth in India is at a historic low and many individuals are actually leaving the job market.[45] In such a situation, any proposed legislation that has the potential to impact firm productivity and the labor market requires careful analysis before it is enacted into law. If the proposed bill does have significant negative implications for small businesses—through increased compliance costs, for example—it could potentially undermine a number of measures that the Indian government has taken to encourage the growth of SMEs in the past few years.[46]

Careful analysis of the impact of the proposed bill on emerging technologies and their applications in the Indian context is also needed. For example, the proposed bill could potentially impact the business models of many firms providing financial technology (or fintech) services.[47] These fintech firms rely on emerging technology (like machine learning) to cut customer on-boarding and servicing costs,[48] which enables them to combat India's problem of financial exclusion. Consequently, requirements in the proposed bill that could potentially inhibit the growth of such services in the Indian economy need to be carefully evaluated.

To conclude, the specific design of institutional choices that India adopts for data protection is likely to have a significant impact on India's economy. These consequences could be direct (such as increased compliance costs) or indirect (the potential stifling of innovation, and overall productivity losses). While the numerical estimates discussed may not necessarily hold true with respect to India, they do highlight the disparate ways in which a GDPR-style data protection law could impact certain sectors of the Indian economy. In doing so, they also emphasize the urgent necessity for careful economic analysis of the data protection bill proposed by the DPC.

ABOUT THE AUTHOR

Anirudh Burman is a senior research analyst at Carnegie India. He works on key issues relating to public institutions, public administration, the administrative and regulatory state, and state capacity.

NOTES

1 European Commission, "2018 Reform of EU Data Protection Rules," Text, European Commission, accessed March 7, 2019, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

2 Tamara Evdokimova, "New Bill From Elizabeth Warren Proposes Potential Jail Time for CEOs for Massive Consumer Data Breaches," *Slate Magazine*, April 5, 2019, https://slate.com/technology/2019/04/elizabeth-warren-equifax-cambridge-analytica-regulation-data-privacy.html.

3 Committee of Experts under the Chairmanship of Justice B N Srikrishna, "Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna," Committee Report (India: Ministry of Electronics & Information Technology, Government of India, July 27, 2018), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf. See Office Memorandum constituting the Committee provided in Annexure A of the report.

4 Committee of Experts under the Chairmanship of Justice B N Srikrishna, "Draft Personal Data Protection Bill, 2018," July 27, 2018, https://www.thehinducentre.com/resources/article24561526.ece/binary/Personal_Data_Protection_Bill,2018_0.

5 "The Information Technology Act, 2000," Government of India, June 9, 2000, https://meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf.

6 "Justice KS Puttaswamy and Another Vs. Union of India and Ors," 10 SCC 1, Supreme Court of India, 2017, https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

7 See paragraph 185 of the judgement by the plurality of judges authored by J. Chandrachud in "Justice KS Puttaswamy And Another Vs. Union of India and Ors," 10 SCC. https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

8 See clause 2(32) of the "Draft Personal Data Protection Bill," which defines "processing," and clause 2(14), which defines "data principal."

9 "Draft Personal Data Protection Bill," clauses 8, 12.

10 "Draft Personal Data Protection Bill," clauses 4–5, 10.

11 "Draft Personal Data Protection Bill," clauses 15–23 and 35–36.

12 "Draft Personal Data Protection Bill," clauses 26, 27.

13 "Draft Personal Data Protection Bill," clauses 40, 41.

14 "Draft Personal Data Protection Bill," clause 60.

15 "Draft Personal Data Protection Bill," clauses 65, 69–73.

16 "Draft Personal Data Protection Bill," clauses 90–92.

17 "Draft Personal Data Protection Bill," clause 3(13).

18 Clause 1(3) of the Bill states that it will apply to foreign business providers if they process data in connection to any business in India, have any "systematic activity of offering goods and services to Indian data principals," or if the processing requires the profiling of data principals within the territory of India.

19 European Parliament, "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," Pub. L. No. Official Journal L 281, 0031, 1995, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX-:31995L0046:en:HTML.

20 Researchers at the National Institute of Public Finance and Policy have, however, analyzed the impact of the proposed data localization requirements contained in the bill. They argue that localization requirements must be considered carefully on a case-by-case basis, and that there is no clear benefit from adopting localization requirements as proposed in the bill. See, Rishab Bailey and Smriti Parsheera, "Questioning the Means and Ends," NIPFP Working Paper Series, no. 242, October 31, 2018, https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf.

21 European Commission, "Impact Assessment Accompanying the Document - Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Commission Staff Working Paper, 2012, https://ec.europa.eu/transparency/regdoc/rep/2/2012/EN/SEC-2012-72-2-EN-MAIN-PART-1.PDF.

22 European Commission, IA, 12–16.

23 European Commission, IA, 12–30.

24 European Commission, IA, 10.

25 European Commission, IA, section 7, 79–92.

26 UK Ministry of Justice, "Impact Assessment: Proposal for an EU Data Protection Regulation," November 22, 2012, https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf.

27 The UK IA also critiqued the EU GDPR for adopting a methodology that covered only administrative costs, while excluding "other policy costs or compliance costs, or costs to the public sector." See UK Ministry of Justice, IA, 9.

28 UK Ministry of Justice, IA, 13–14.

29 UK Ministry of Justice, IA, Annexure B, "Impact on Small Businesses."

30 European Centre for International Political Economy, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce" March 2013, https://www.uschamber.com/sites/default/files/legacy/reports/020508_EconomicImportance_Final_Revised_lr.pdf.

31 "The Economic Importance of Getting Data Protection Right," 18.
32 Ibid. The right to be forgotten is an obligation on data controllers to remove all personal data.
33 "The Economic Importance of Getting Data Protection Right," 16.
34 Matthias Bauer et al., "The Costs of Data Localisation: Friendly Fire on Economic Recovery," ECIPE Occasional Paper Series, European Centre for International Political Economy, 2014, 10, http://hdl.handle.net/10419/174726.
35 Ibid., 5–9.
36 Martina Francesca Ferracane, Janez Kren, and Eric van der Marel, "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?," European Center for International Political Economy DTE Working Paper, October 2018, https://ecipe.org/publications/do-data-policy-restrictions-impact-the-productivity-performance-of-firms-and-industries/.
37 L. Christensen et al., "The Impact of the Data Protection Regulation in the E.U.," Intertic Working Paper, February 1, 2013, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.138&rep=rep1&type=pdf.
38 Christensen et al., 27.
39 Christensen et al., 31.
40 Christensen et al., 5.
41 Els De Busser et al., "Big Data: The Conflict Between Protecting Privacy and Securing Nations," in "Big Data: A Twenty-First Century Arms Race," Atlantic Council, 2017, 5–16, https://www.jstor.org/stable/resrep03719.5; and Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Seton Hall Law Review* 47 (2017): 26.
42 Els De Busser et al., "Big Data: The Conflict Between Protecting Privacy and Securing Nations;" and Zarsky, "Incompatible: The GDPR in the Age of Big Data," 1003.
43 Matthias Berberich and Malgorzata Steiner, "Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers Reports: Practitioner's Corner," *European Data Protection Law Review* (EDPL) 2, no. 3 (2016): 422–26.
44 See European Commission, IA, 89, for a discussion on the increased costs of compliance of GDPR being offset by harmonization requirements.
45 Mahesh Vyas, "11 Million Jobs Lost in 2018 - One-Third of Them by the Salaried Class," *Business Standard India*, January 7, 2019, https://www.business-standard.com/article/opinion/11-million-jobs-lost-in-2018-119010700554_1.html.
46 Ministry of Micro, Small and Medium Enterprises, Government of India, "Indian MSMEs Marching Ahead: Achievements 2014-18," 2018, https://msme.gov.in/sites/default/files/MSME%20Achievement_English%202014-18.pdf.
47 On the kinds of technological innovations driving the growth of fintech, see Working Group on Fintech and Digital Banking, "Report of the Working Group on FinTech and Digital Banking," November 2017, 7–16, https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF.
48 See Ibid.

CARNEGIE INDIA