DIGITAL PERSONAL DATA PROTECTION BILL, 2022: EXAMINING THE LEGISLATIVE ATTEMPT TO PROTECT PERSONAL DATA IN INDIA?

Rishit*

ABSTRACT

From intellectual circles to tea-stall meetings, there have been a lot of discussions and debates about the lack of intent and initiative from the side of the Government of India ("Centre") regarding data protection and data privacy norms. The European Union ("EU") 's General Data Protection Regulation ("GDPR")[1] came to effect in 2018 and the United States of America ("US") 's American Data Privacy And Protection Act ("ADPPA")[2] introduced in the US Congress on June 21, 2022, are examples which show that demands for such legislation are neither very recent nor local. The more valuable and relevant anything becomes, the more it also becomes prone to exploitation and misuse and as a result, the more protection and caution is required to handle it. And there's hardly anything more valuable and relevant in the 21st century and arguably for centuries to come than data. The same can be summed up neatly in British mathematician Clive Humby's words, "Data is the new oil." In India's context, since the last decade, we are quickly moving towards a "digitised India." Mobile users and internet subscribers are literally increasing every day with recent estimates putting the number at 700 million.[3] With the increased use of cyber facilities, cybercrimes are also increasing. That makes data protection very essential. Therefore, the Digital Personal Data Protection Bill, 2022 ("the Bill") is a welcome initiative coming from the Centre but it's not without its limitations. This article will attempt to highlight these limitations and present possible solutions.

BACKGROUND

The first initiative towards data protection in India was the rules made in 2011 under the IT Act, of 2000[4] but they were found to be inadequate and specific legislation for data protection

*BA LLB, SECOND YEAR, NATIONAL LAW UNIVERSITY, JODHPUR.
[1]General Data Protection Regulation [2016], Regulation (EU) 2016/679.
[2]American Data Privacy and Protection Act 2022.
[3]ShilpaRanipeta, 'There are over 700 million internet users in India — and just as many who don't use it'(*CNBC-TV18*,28 July 2022) https://www.cnbctv18.com/technology/iamai-kantar-report-says-rural-india-accounts-for-more-than-half-the-internet-users-in-country-14283262.html accessed 10 June 2023.
[4]Information Technology Act 2000, s 43A.

was demanded. The real traction in the demand for such a bill came about after the Supreme Court's judgement of *Justice K. S. Puttaswamy&Anr. vs Union Of India &Ors.*[5]which recognised the right to privacy as a part of the right to life and personal liberty under Article 21 of the Indian Constitution[6]. Following the decision, the apex court directed the Centre to enact a statute containing rules The first attempt at a digital data protection act was in 2017[7] and the last one was in 2019[8]. In 2019, the Justice B.N. Srikrishna Committee prepared the draft for a data protection bill and presented it in Parliament but it was criticised on different and even contrasting grounds by different stakeholders. For example, technology companies found the provisions regarding data localisation too stringent while civil society organisations and netizens pointed out that the penalties for privacy violations weren't stringent enough to create a sense of deterrence among potential violators. Following the Joint Parliamentary Committee's recommendation for extensive changes, the Centre decided to withdraw the bill from Parliament and present a new one.[9]

The new Bill under discussion is the fourth attempt toward statutory protection of digital personal data by the legislature. An attempt has been made to make it more comprehensive than the earlier versions and that shows. According to the MEITY, "the Digital Personal Data Protection Bill is a legislation that frames out the rights and duties of the citizen (Digital Nagrik) on the one hand and the obligations of the Data Fiduciary to use collected data lawfully on the other."[10] The bill's provisions revolve around three stakeholders: the data principal (the individual whom the data pertains to, or his parent or guardian if the individual is under the age of 18), the data fiduciary (the one who determines the object and way of processing personal data), and the grievance resolver (the bill proposes to establish a body called the Data Protection Board of India for the same).

According to Rajeev Chandrasekhar, an IT minister states the European General Data Protection Regulation is looked up to for setting the highest standard for data protection but he called upon India to create its own path and build a framework made keeping the Indian

[5]*Justice K. S. Puttaswamy&Anr. v Union Of India &Ors*(2017) 10 SCC 1.
[6]The Indian Constitution 1950, art 21.
[7] Data (Privacy and Protection) Act 2017.
[8] Personal Data Protection Act 2019.
[9]Mihir Nigam, 'The Digital Personal Data Protection Bill, 2022 suffers from flaws which may render it unconstitutional'(*The Leaflet*, 2December, 2022)https://theleaflet.in/the-digital-personal-data-protection-bill-2022-suffers-from-flaws-which-may-render-it-unconstitutional/accessed 10 June 2023.
[10]Payal Mehta, 'Govt likely to bring Data Protection Bill in next year's Budget Session'*Economic Times* (New Delhi, 03December 2022).

scenario in mind.[11] This seems to have been done to a large extent. The bill while drawing significant inspiration from data protection norms around the globe like the GDPR, improves upon them. For example, unlike the GDPR, it provides definitions for the terms "harm", "loss", and "public interest". In another welcome move, the bill uses “her” and “she” to refer to an individual.

Although the bill does a better job compared to its previous iterations when it comes to striking a balance between protecting people’s data and allowing data fiduciaries reasonable access to it and also when it comes to addressing certain essential aspects of protecting digital data like data compliance, the right to be forgotten, cross-border data flows, etc, does the bill have the right standing to protect our digital data? Not in its current shape. There are some major red flags in the bill that need to be addressed before it is presented in Parliament.

On the Data Protection Board of India

First, the bill establishes an entity called the Data Protection Board of India to impose penalties on violators of the Act.[12] This sounds ideal but there’s a catch. In a downgrade from a previous version of the bill which sought to establish the Board as a statutory authority, the current version vests this function completely with the Centre. The provisions of the bill instead of making this entity as independent in its functioning as possible so as to ensure its unbiased and smooth working that ensures the protection of people’s data and penalisation of violators, reduce it to the level of a government puppet and a token body. The Centre has given itself an unfair degree of control in the appointment, removal and functioning of the members of the Board with the appointment of the Chairperson and other members being entirely at the discretion of the Centre.[13] The body needs to be independent to be able to ensure the protection of people’s personal data from everyone including government entities which it clearly isn’t capable of doing in its current state as its dependence on the Centre will give government entities a free pass to deal recklessly with people’s personal data or even misuse it. Although section 22(2) of the bill upholds judicial review by providing that the decisions of the Board can be appealed against in High Courts, on the flip side, there’s a high chance that it will lead to many appeals being filled on the ground that the Board is biased

[11]Kavita Chowdhury, ‘India’s Controversial Data Protection Bill’(*The Diplomat*,20December 2022)https://thediplomat.com/2022/12/indias-controversial-data-protection-bill/accessed 10 June 2023.
[12]The Digital Personal Data Protection Bill 2022, s 19(1).
[13] The Digital Personal Data Protection Bill 2022, s 19(2).

towards the government in its decisions.[14]In order to avoid such appeals, the body must be self-contained. One can't disagree that the Centre needs to have the required means to ensure the security, sovereignty, and integrity of India and the maintenance of public order but the exemptions it has given itself go too far and are vague in nature. Vague provisions, an inefficient citizen recourse process and keeping the government on a pedestal defeat the purpose of the bill by absolving the Centre's accountability and facilitating mass surveillance. Thus, the Board needs to be made independent and it's functioning efficiently. Also, won't it make sense to subject the data collected by the Board as a part of its functioning to the same provisions as any other data to ensure that it's protected too? Is there any point to "No suit, prosecution or other legal proceedings shall lie against the Board or its Chairperson, Member, employee or officer for anything which is done or intended to be done in good faith under the provisions of this Act?"[15] Or is it just the government shielding its puppet Board from accountability?

On Data Localisation

Second, as a departure from its previous iterations, the norms regarding data localisation have been relaxed. This is also a departure from the trend seen in recent years where there has been a huge emphasis on local storage of data with the Draft E-Commerce Policy making data localisation mandatory for big corporate companies[16] and the Reserve Bank of India making it mandatory to store people's payment data locally.[17]While this comes as a sigh of relief for technology firms, at the same time the Centre needs to clarify (through amendments in the bill, if necessary), to people how it's going to ensure no comprise takes place when it comes to the security of people's data to avoid any reservations regarding the relaxations.

On Cross-border Data Flow

Third, safeguarding people's digital data when it comes to cross-border data flow is more relevant today than ever because as a result of India's increasing relevance and importance in the global order, the past few years have seen an unprecedented no. of Free Trade Agreements (FTA) and Regional Trade Agreements (RTA) being discussed, negotiated

[14]The Digital Personal Data Protection Bill 2022, s 22(2).
[15] The Digital Personal Data Protection Bill 2022, s 19(6).
[16]Shashidhar K.J., 'India's draft e-commerce policy: A need to look beyond data as the new oil'(*Observer Research Foundation*,30 March 2019) https://www.orfonline.org/expert-speak/indias-draft-e-commerce-policy-a-need-to-look-beyond-data-as-the-new-oil-49413/accessed 10 June 2023.
[17]Nikhat Hetavkar, 'Payments data must be stored in systems located in India, says RBI'*The Business Standard*(Mumbai, 27 June 2022).

and signed and the same continues to happen[18] which makes it essential to ensure Data Free Flow with Trust (DFFT) and secured cross-border data flows. Under the bill's definition of "public interest", "friendly relations with foreign states"[19] and "preventing the dissemination of false statements of fact"[20] have been added to ensure this. The Centre has been given the power to specify via notification the countries where India's personal data can reside[21] but no recourse has been provided in the situation when relations deteriorate with a previously notified country or if such a country's standard of handling digital data deteriorates to the point that it becomes unsafe to share our data with them anymore. A bigger issue is that the Centre has reserved wide and sweeping powers for itself to exempt entities involved in cross-border data transfer which is a big cause for concern as it creates the possibility of people's personal data going into the wrong hands if it's left to the government's whims with no accountability.[22]Article 44 to 50 of the GDPR permits digital personal data transfer belonging to EU's Data Principals only to those countries which maintain a satisfactory standard of data protection.[23] A similar provision should be inserted in the Bill through an amendment.

On Non-Personal Data

Fourth, the earlier iterations of the bill distinguished between and had separate provisions for handling non-personal data but the current one solely focuses on personal data and doesn't even mention anything about data that is non-personal in nature. This leaves open the possibility of unregulated exploitation of non-personal data by data fiduciaries.

On Exemptions and Powers Given to the Centre

Fifth, the Centre has availed itself and its agencies with wide-ranging exemptions while dealing with people's personal data with little to no safeguards which creates the possibility of misuse and manipulation by these agencies using this data.[24] The Centre has been given the authority to give leeway to its subordinate bodies from adhering to the provisions of the

[18]PIB Delhi, 'India has signed 13 Regional Trade Agreements (RTAs)/Free Trade Agreements (FTAs) with various countries/regions'*Press Information Bureau*(New Delhi, 20 July 2022).
[19]The Digital Personal Data Protection Bill 2022,s2(18)(c).
[20] The Digital Personal Data Protection Bill 2022, s 2(18)(f).
[21] The Digital Personal Data Protection Bill 2022, s 17.
[22]The Digital Personal Data Protection Bill 2022, s 18(1).
[23]General Data Protection Regulation [2016], Regulation (EU) 2016/679, art 44-50.
[24] The Digital Personal Data Protection Bill 2022, s 18.

bill through notification for national security reasons.[25] Such disproportional exemptions violate the judgement of *K.S. Puttaswamy v Union of India* which made it clear that any state interference in people's privacy must stand the test of legality, necessity and proportionality.[26]Governments have time and again used the excuse of national security to justify their questionable conduct so it will not be surprising if the same is done in this case as well. The phrase "as may be prescribed" has been used 18 times in the bill which means a lot which could have easily been settled in the bill has simply been left to the Centre's discretion. Multiple proven and unproven allegations have been made against every political regime in the past and present regarding misuse of personal data and improper ways of collecting personal data and such wide-ranging exemptions will only give way to more of these allegations in the future, defeating the purpose of this bill and eroding the public's trust in the government with regard to handling their data. In the case of *People's Union for Civil Liberties v. Union of India*, it was held by the SC that the state can only interfere in people's privacy in the event of a "public emergency" or in the "interest of public safety." The court described public emergency as "the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action" and public safety as "the state or condition of freedom from danger or risk for the people at large."[27] Such clarifying definitions need to be incorporated into the Bill and adhered to if the government wishes to interfere with people's privacy when it genuinely needs to in the best interest of the country without any eyebrows being raised from the public against it because even if the Centre is able to pass the bill as it is if its validity is questioned in the court, it's likely to be declared null and void for over-empowering the Centre without proper checks and balances and violating the SC judgements mentioned above.

On Action against Violators

Sixth, there's a disproportionate focus on the severity of the violation rather than the violation itself. It has been provided that if the non-compliance isn't significant, the Board has the discretion to close the inquiry.[28] The use of the word "significant" is vague and subjective and is open to exploitation. The Board should be allowed to impose penalties based on the degree of violation and not only when it's "significant." In addition, the bill calls for a hefty

[25] The Digital Personal Data Protection Bill 2022, s 18(2).
[26] *Justice K. S. Puttaswamy&Anr. vs Union Of India &Ors*(2017) 10 SCC 1.
[27] *People's Union for Civil Liberties v. Union of India*(2013) 10 S.C.C. 1.
[28] The Digital Personal Data Protection Bill 2022, s 21(11).

penalty on significant noncompliance "not exceeding Rs. 500 crores in each instance."[29] A better option would be to have a ramp-based penalty system as it would kill two birds with one stone i.e. it won't have any negative impact on the world's 3rd largest start-up ecosystem and it will also provide the required deterrence against violating the bill's provisions. The Centre can take inspiration from China which imposes penalties based on the firm's size and turnover.[30] Another major issue is that the violations have only been subjected to financial penalties and no criminal convictions. This is akin to putting a price on an individual's privacy and making it open for purchase by any big shot willing to pay for it.

On Missing Provisions

Seventh, the bill should specify the time period till which digital personal data can be processed and retained, and such duration must be communicated to data principals by data fiduciaries when obtaining their consent to process data. It should also specify the process of destruction of the retained data and the data principals have to be informed when the data has been destroyed. Taking a leaf from the California Consumer Privacy Act, 2018, the data fiduciaries shall be mandated to take consent from the data principals separately for sharing their data with third parties or for cross-border data transfer.[31] The bill's silence on such matters can easily be exploited by data fiduciaries in their favour.

On Protecting Children's Data

Eighth, the Centre should consider the suggestion by the global trade association Information Technology Industry Council (ITI) on reconsidering the provision of blanket prohibitions on tracking, monitoring behaviour and targeted advertisements for protecting children's data and reducing it to only the processing of such data that has the potential to cause harm, because, as has been reasoned by them such extreme restrictions can deprive them of accessing a lot of useful content and prevent service providers from blocking inappropriate content.[32]

[29]The Digital Personal Data Protection Bill 2022, s 25(1).
[30]Kirti Bhargava, 'Explained: Concerns Over The New Data Protection Bill And How It Is Different From 2019 Draft' *Outlook India*(New Delhi, 21 November2022).
[31] The California Consumer Privacy Act, 2018, s 120(b).
[32]Press Trust of India, 'Government's New Data Protection Bill To Hit Investments In Data Centres' (*NDTV*, 27 December 2022) https://www.ndtv.com/business/significant-controls-to-govt-under-data-protection-bill-to-hit-investments-in-data-centres-3641090 accessed 10 June 2023.

On omitting Section 8(1)(j) of the RTI Act

Ninth, Section 30(2)[33]amends Section 8(1)(j) of the RTI Act[34]which is one of the exceptions to disclosing information under it. It provides that information that isn't related to public interest or disclosure which would amount to invasion of an individual's privacy shall not be disclosed. It also seeks to omit its proviso which provides that any information which can't be denied to a Legislature or the Parliament also can't be denied to an individual too. Why would a bill intended to protect personal data intend to amend/omit such provisions? It would weaken the transparency and effectiveness of its own intended outcome i.e. protecting people's data.

CONCLUSION

The bill gets certain things right but leaves much to be desired. Only a just, fair and reasonable law can protect the citizen's digital personal data and further their fundamental rights while giving reasonable scope of interference to the Centre and ensuring that the growth of the corporate sector in India continues – all at the same time. Such a bill has to steer clear of all sorts of vagueness, arbitrariness and high-handedness. It has to keep all data fiduciaries on the same ground and subject their actions to an independent and sturdy body. To achieve all this, the Centre has to take into account all the genuine recommendations and concerns and make suitable changes where required before the bill is tabled in Parliament, which is much easier to do than bringing out a fifth iteration later on.

[33] The Digital Personal Data Protection Bill 2022, s 30(2).
[34] The Right to Information Act 2022, s 25(1).