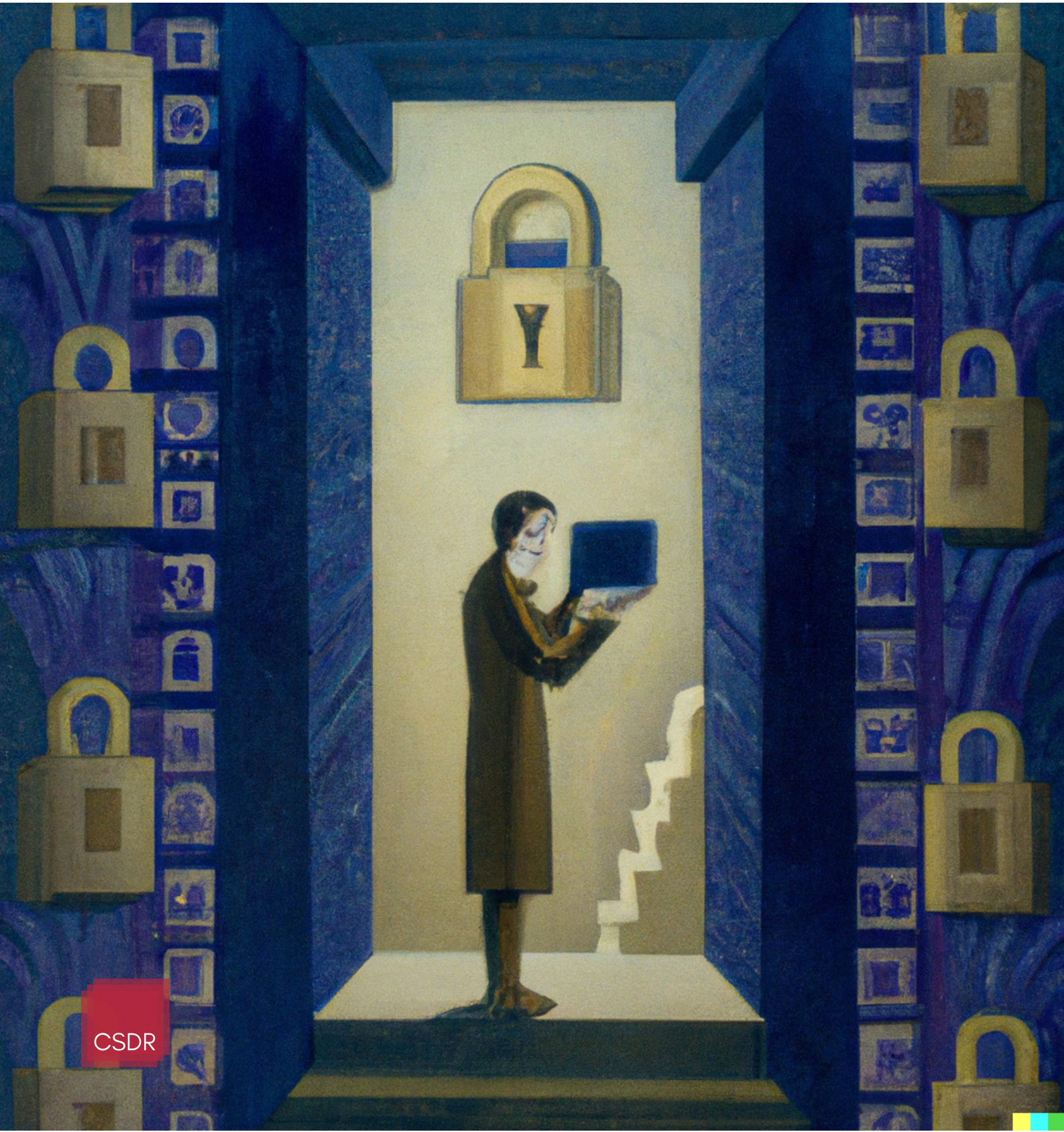
India's Digital Personal Data Protection Bill 2022

CSDR's feedback submitted to MeitY



INTRODUCTION

On 18 November 2022, the Indian government published the draft Digital Personal Data Protection Bill (2022). This was the fourth iteration of an ambitious data protection law first introduced in 2018. Since then, its nomenclature and scope have changed to a large extent. The bill, since its inception, has been focused on personal data, except for the previous version (The Data Protection Bill, 2021) that widened its scope to non-personal data. India has been keen on implementing a data protection regime to govern its growing internet market.

Several attempts have been made since the landmark Supreme Court judgement in 2017 which declared the right to privacy as a fundamental right. Notably, it has also done away with data localization which requires data fiduciaries to store data within the country. Instead, the government will notify—under yet unspecified criteria—countries and territories outside India where data can be transferred.

The Ministry of Electronics and Information Technology invited public feedback on the draft bill, the deadline for which was 2 January 2023. The Council for Strategic and Defense Research (CSDR) identified three problem areas in the draft bill and submitted feedback on them. Our feedback was drafted by in-house experts who consulted multiple stakeholders including rights activists, policy analysts, defense experts, advocates, academicians and technical experts.

CSDR conducted a closed-door group discussion with the stakeholders to focus on the issues of cross-border data transfers, exemptions granted to the government and private data fiduciaries, and the composition and functions of the Data Protection Board.

Our feedback highlighted the need for elaborating guiding principles for data transfers outside India. The pre-defined principles will serve our twin goals of signing bilateral agreements for digital trade and meeting data access requirements of security agencies. Exemptions granted to the government under broad and ambiguous criteria will expose the bill to litigation challenges owing to its non-compliance with the Puttaswamy judgement (given the absence of safeguards and proportionality).

The bill also allows the government to grant exemptions to a data fiduciary or a class of data fiduciaries based on the "volume and nature of personal data processed". This provision was flagged as problematic since it can potentially hurt the rights of the users and lead to lobbying efforts by private entities. Our feedback also pointed out the need for an independent data protection authority with certain key functions (defined within the law) given that this bill leaves it to the Central Government to decide on the composition and functioning of the Data Protection Board.

CHAPTER 4 (SPECIAL PROVISIONS)

SECTION 17 (TRANSFER OF PERSONAL DATA OUTSIDE INDIA)

Section 17 of the bill allows the central government to notify countries/territories outside India to which a data fiduciary can transfer personal data. The assessment to decide on the permissibility of data transfer will be conducted based on unspecified "terms and conditions".

ISSUES AND RECOMMENDATIONS

Section 17 can allow the Government to sign bilateral trade agreements for data sharing. A trusted geography approach will provide space for negotiation and create better, and customizable, data sharing opportunities with the partner countries. However, section 17 leaves significant gaps in terms of defining the assessment criteria for notifying countries. It does not provide clarity on whether all the countries are, by default, whitelisted or blacklisted for data transfer. The inability of a country to qualify for data transfer may again lead to data localization and harm Indian startups. Since the bill empowers the government to make rules for cross-border data sharing and does not specify any guiding principles for the process, a change in the government may also lead to a change in these principles; this will dilute India's bargaining power internationally. The bill, therefore, lacks the dynamism and permanency required of a data protection law. The absence of guiding principles also makes it difficult for a foreign government to initiate negotiations with India for a data sharing agreement.

The principles are essential for India to sign such an agreement with a foreign government, as they will need to have some understanding of India's expectations to decide on the agreement.

It is recommended that the government publish a policy document to define a set of guiding principles for data transfers abroad. The guiding principles may also be made part of the bill itself. The principles may include protection of Indian citizen data from foreign surveillance, access to data for law enforcement when required and other requirements which earlier motivated the Central Government towards data localization. India's earlier focus on data localization stemmed from the perception that it will lead to innovation. However, on the contrary, not being able to transfer data to regions outside India may impede Indian businesses which currently leverage cloud and computing services provided by international service providers. The ambiguity in defining principles for data transfer and leaving them to evolve under bilateral agreements is also problematic. A lack of uniformity will also make it difficult for foreign technology companies to invest in or shift operations to India. Therefore, it is in India's economic interest to pre-define common underlying principles for cross-border data transfers while leaving room to negotiate individual bilateral agreements.

SECTION 18 (EXEMPTIONS)

Section 18 enables the Central Government to exempt "any instrumentality of the state" and "certain or a class of data fiduciary" from the application of this legislation. The exemption to state instrumentality can be granted "in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these". The section has dropped the mention of "just, fair and reasonable" procedures to be followed by the government.

ISSUES AND RECOMMENDATIONS

In terms of establishing "proportionality" of government action against the fundamental right to privacy, the safeguards mentioned by the Puttaswamy judgement include "the extent of such interference must be proportionate to the need for such interference" and "procedural guarantees against abuse of such interference". These safeguards are missing from the bill's current draft, exposing the legislation and the orders passed under it to litigation challenges. For example, sub-section (4) of section 18 allows the government to retain data indefinitely. However, according to the Puttaswamy judgement, purpose limitation and data minimization would be the ideal way to ensure that the principle of proportionality is met.

The bill also allows the Central Government to grant exemptions to a data fiduciary or a class of data fiduciaries from Section 6, sub-sections (2) and (6) of section 9, sections 10, 11 and 12 of the bill.

The bill mentions "volume and nature of personal data processed" as criteria to decide on these exemptions; the under-defined provision will lead to lobbying efforts by private entities who will attempt to influence policy making in their favour.

It is recommended that the bill finds a balance to meet the proportionality test by defining procedures for granting exemptions; the procedure should specify the class of data and time period with respect to the scope of activities, and purpose for the exemptions. This must be done under judicial oversight to ensure that data access by government entities meets constitutional standards. Definitions of national security and public order must be clarified to help with the procedures. The procedure and the definitions have to be tailored to the extent that they allow for a case-by-case evaluation for proportionality.

The Central Government has specified exemptions to a certain or class of data fiduciaries to facilitate early-stage Indian start-ups and reduce compliance burden. We recommend that the exemptions be granted to start-ups listed under the MSME Development Act, 2006.

CHAPTER 7 (COMPLIANCE FRAMEWORK)

SECTIONS 19 AND 20 (DATA PROTECTION BOARD AND ITS FUNCTIONS)

Section 19 says that the Data Protection Board's (DPB) composition, strength, the process of selection, terms and conditions of appointment and service and removal of its chairperson and other members have been left to be prescribed for later by the Central Government. The Central Government will decide the conditions of appointment and service for the chief executive, other board officers, and members.

Section 20 says that the DPB will "determine non-compliance" with the act and impose penalties under its provisions. It is also supposed to "perform such functions as the Central Government may assign" to it.

ISSUES AND RECOMMENDATIONS

The data protection authority was envisaged as a rule-making specialised body in the previous versions of the bill. The body was given legislative, executive and adjudicatory powers. The current bill leaves the role of the DPB open-ended as its powers are not clear. The DPB will determine non-compliance, impose penalties and perform functions as the Central Government may decide later; the functions to be undertaken by the Board have not been defined. This creates a problem as the members of the Board will lack necessary details to perform any such functions. The ambiguity also means that there is no clarity on how the board will cooperate with other sectoral regulators, such as the RBI and the TRAI.

The Board's composition and appointment are left to be decided by the central government, casting apprehensions on its autonomy. The government itself is one of the largest data fiduciaries in the country and, therefore, cannot be expected to regulate itself. A data protection body which lacks the globally-accepted principle of impartiality will be an obstacle in cross-border data flows to regions, such as Europe, where strict data protection laws are operational.

It is recommended that the bill defines the exact functions and powers of the DPB for parliamentary scrutiny. As the Sri Krishna Committee recommended, the regulatory body should have the power to monitor, enforce, investigate, research, generate awareness and set standards. Further, codes of practice and categorising data fiduciaries can be used to achieve enforcement objectives. In addition to the adjudicatory role, the board must also have an advisory role, where it can take inputs from all the stakeholders for policy making. A sub-law can be brought in to facilitate intersectoral cooperation.

The DPB can adopt a structure on the lines of the Consumer Protection Council to ensure the board's independence; the members and chairpersons must have fixed tenure, post-retirement safeguards, restriction on future employment and financial independence; the composition includes members with technical and legal expertise to fulfil the board's broader objectives.

3, PRATAP SINGH BUILDING
JANPATH LANE, NEW DELHI
INDIA - 110001

PHONE: 011-43104566
EMAIL: OFFICE@CSDRONLINE.ORG
WEB: WWW.CSDRONLINE.ORG
TWITTER: @CSDR_INDIA