General Comments to the Personal Data Protection Bill 2019

Comments and Recommendations

20 February, 2020

By **Amber Sinha**, **Elonnai Hickok**, **Pallavi Bedi**, **Shweta Mohandas** and **Tanaya Rajwade**

The Centre for Internet and Society, India

General Comments

1. *Executive notification cannot abrogate fundamental rights*

In 2017, the Supreme Court in *K.S. Puttaswamy v Union of India*[1] held the right to privacy to be a fundamental right. While this right is subject to reasonable restrictions, the restrictions have to meet a three fold requirement, namely (i) existence of a law; (ii) legitimate state aim; (iii) proportionality.

Under the 2018 Bill, the exemption to government agencies for processing of personal data from the provisions of the Bill in the '*interest of the security of the State*'[2] was subject to a law being passed by Parliament. However, under Clause 35 of the present Bill, the Central Government is merely required to pass a written order exempting the government agency from the provisions of the Bill.

Any restriction on the right to privacy will have to comply with the conditions prescribed in Puttaswamy I. An executive order issued by the central government authorising any agency of the government to process personal data does not satisfy the first requirement laid down by the Supreme Court in *Puttaswamy I* — as it is not a law passed by Parliament. The Supreme Court while deciding upon the validity of Aadhar in *K.S. Puttaswamy v Union of India*[3] noted that *"an executive notification does not satisfy the requirement of a valid law contemplated under Puttaswamy. A valid law in this case would mean a law passed by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental right cannot be sustained by an executive notification."*

2. *Exemptions under Clause 35 do not comply with the legitimacy and proportionality test*

The lead judgement in Puttaswamy I while formulating the three fold test held that the restraint on privacy emanate from the procedural and content based mandate of Article 21.[4] The Supreme Court in *Maneka Gandhi v Union India*[5] had clearly established that *"mere prescription of some kind of procedure cannot ever meet the mandate of Article 21. The procedure prescribed by law has to be fair, just and reasonable, not fanciful, oppressive and arbitrary."*[6]

The existence of a law is the first requirement; the second requirement is that of 'legitimate state aim'. As per the lead judgement this requirement ensures that *"the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action."*[7] It is established that for a provision which confers upon the executive or administrative authority discretionary powers to be regarded as non-arbitrary, the provision should lay down clear and specific guidelines for the executive to exercise the power.[8]

The third test to be complied with is that the restriction should be 'proportionate,' i.e. the means that are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. The Supreme Court in *Modern Dental College & Research Centre v State of Madhya Pradesh*[9] specified the components of proportionality standards —

i. A measure restricting a right must have a legitimate goal;
ii. It must be a suitable means of furthering this goal;
iii. There must not be any less restrictive, but equally effective alternative; and
iv. The measure must not have any disproportionate impact on the right holder

Clause 35 provides extensive grounds for the Central Government to exempt any agency from the requirements of the bill but does not specify the procedure to be followed by the agency while processing personal data under this provision. It merely states that the 'procedure, safeguards and oversight mechanism to be followed' will be prescribed in the rules.

The wide powers conferred on the central government without clearly specifying the procedure may be contrary to the three fold test laid down in Puttaswamy I, as it is difficult to ascertain whether a legitimate or proportionate objective is being fulfilled.[10]

3. *Limited powers of Data Protection Authority in comparison with the Central Government*

In comparison with the last version of the Personal Data Protection Bill, 2018 prepared by the Committee of Experts led by Justice Srikrishna, we witness an abrogation of powers of the Data Protection Authority (Authority), to be created, in this Bill. The powers and functions that were originally intended to be performed by the Authority have now been allocated to the Central Government. For example:

i. In the 2018 Bill, the Authority had the power to notify further categories of sensitive personal data. Under the present Bill, the Central Government in consultation with the sectoral regulators has been conferred the power to do so.
ii. Under the 2018 Bill, the Authority had the sole power to determine and notify significant data fiduciaries, however, under the present Bill, the Central Government has in consultation with the Authority been given the power to notify social media intermediaries as significant data fiduciaries.

In order to govern data protection effectively, there is a need for a responsive market regulator with a strong mandate, ability to act swiftly, and resources. The political nature of the personal data also requires that the governance of data, particularly the rule-making and adjudicatory functions performed by the Authority are independent of the Executive.

4. *No clarity on data sandbox*

The Bill contemplates a sandbox for "innovation in artificial intelligence, machine-learning or any other emerging technology in public interest." A Data Sandbox is a non-operational environment where the analyst can model and manipulate data inside the data management system. Data sandboxes have been envisioned as a secure area where only a copy of the company's or participant companies' data is located.[11] In essence, it refers to the scalable and creation platform which can be used to explore an enterprise's information sets. On the other hand, regulatory sandboxes are controlled environments where firms can introduce innovations to a limited customer base within a relaxed regulatory framework, after which they may be allowed entry into the larger market after meeting certain conditions. This purportedly encourages innovation through the lowering of entry barriers by protecting newer entrants from unnecessary and burdensome regulation. Regulatory sandboxes can be interpreted as a form of responsive regulation by governments that seek to encourage innovation – they allow selected companies to experiment with solutions within an environment that is relatively free of most of the cumbersome regulations that they would ordinarily be subject to, while still subject to some appropriate safeguards and regulatory requirements. Sandboxes are regulatory tools which may be used to permit companies to innovate in the absence of heavy regulatory burdens. However, these ordinarily refer to burdens related to high barriers to entry (such as capital requirements for financial and banking companies), or regulatory costs. In this Bill, however, the relaxing of data protection provisions for data fiduciaries could lead to restrictions of the privacy of individuals. Limitations to fundamental rights on grounds of 'fostering innovation' is not a constitutional tenable position, and contradict the primary objectives of a data protection law. As the government continues to explore frameworks for innovation, it will be important that it coordinates with sectoral regulators to ensure harmonization. For example, The RBI has established a sandbox for banking sector[12] and TRAI has explored setting up a sandbox for the Telecom sector.[13]

5. *The primacy of 'harm' in the Bill ought to be reconsidered*

While a harms based approach is necessary for data protection frameworks, such approaches should be restricted to the positive obligations, penal provisions and responsive regulation of the Authority. The Bill does not provide any guidance on either the interpretation of the term 'harm,'[14] or "significant harm"[15] or on the various activities covered within the definition of the term. Terms such as 'loss of reputation or humiliation' 'any discriminatory treatment' are a subjective standard and are open to varied interpretations. This ambiguity in the definition will make it difficult for the data principal to demonstrate harm and for the DPA to take necessary action as several provisions are based upon harm being caused or likely to be caused. This is particularly concerning as the Bill envisions a tiered approach to harms - "harm" and "significant harm".Some of the significant provisions where 'harm' is a precondition for the provision to come into effect are —

i. **Clause 25:** Data Fiduciary is required to notify the Authority about the breach of personal data processed by the data fiduciary, if such breach **is likely to cause harm** to any data principal. The Authority after taking into account the severity of the harm that may be caused to the data principal will determine whether the data principal should be notified about the breach.

ii. **Clause 32 (2):** A data principal can file a complaint with the data fiduciary for a contravention of any of the provisions of the Act, **which has caused or is likely to cause 'harm'** to the data principal.

iii. **Clause 64 (1):** A data principal who **has suffered harm** as a result of any violation of the provision of the Act by a data fiduciary, has the right to seek compensation from the data fiduciary.

Clause 16(5): The guardian data fiduciary is barred from profiling, tracking or undertaking targeted advertising directed at children and undertaking any other processing of personal data that can cause **significant harm** to the child.

6. *Non personal data should be outside the scope of this Bill*

Clause 91(1) states that the Act does not prevent the Central Government from framing a policy for the digital economy, in so far as such policy does not govern personal data. The Central Government can, in consultation with the Authority, direct any data fiduciary to provide any anonymised personal data or other non-personal data to enable better targeting of delivery of services or formulation of evidence based policies in any manner as may be prescribed.

It is concerning that the data protection bill has specifically carved out an exception for the Central Government to frame policies for the digital economy and seems to indicate that the government plans to freely use any and all anonymized and/or non-personal data that rests with any data fiduciary that falls under the ambit of the bill to support the digital economy including for its growth, security, integrity, and prevention of misuse. It is unclear how the government, in practice, will be able to compel organizations to share this data. Further, there is a lack of clarity on the contours of the definition of non-personal data and the Bill does not define the term. It is also unclear whether the Central Government can compel the data fiduciary to transfer/share all forms of non-personal data and the rights and obligations of the data fiduciaries and data principals over such forms of data. Anonymised data refers to data which has 'irreversibly' been converted into a form in which the data principal cannot be identified. However, as several instances have shown 'irreversible' anonymisation is not possible. In the United States, the home addresses of taxi drivers were uncovered and in Australia individual health records were mined from anonymised medical bills.[16]

In September 2019, the Ministry of Electronics and Information Technology, constituted an expert committee under the chairmanship of Kris Gopalkrishnan to study various issues relating to non-personal data and to deliberate over a data governance framework for the regulation of such data.

The provision should be deleted and the scope of the bill should be limited to protection of personal data and to provide a framework for the protection of individual privacy. Until the report of the expert committee is published, the Central Government should not frame any law/regulation on the access and monetisation of non-personal/anonymised data nor can they create a blanket provision allowing them to request such data from any data fiduciary that falls within the ambit of the bill. If the government wishes to use data resting with a data fiduciary; it must do so on a case to case basis and under formal and legal agreements with each data fiduciary.

7. *Steps towards greater decentralisation of power*

We propose the following steps towards greater decentralisation of powers and devolved jurisdiction —

i. **Creation of State Data Protection Authorities:** A single centralised body may not be the appropriate form of such a regulator. We propose that on the lines of central and state commissions under the Right to Information Act, 2005, state data protection authorities are set up which are in a position to respond to local complaints and exercise jurisdiction over entities within their territorial jurisdictions.

ii. **More involvement of industry bodies and civil society actors:** In order to lessen the burden on the data protection authorities it is necessary that there is active engagement with industry bodies, sectoral regulators and civil society bodies engaged in privacy research. Currently, the Bill provides for involvement of industry or trade association, association representing the interests of data principals, sectoral regulator or statutory Authority, or an departments or ministries of the Central or State Government in the formulation of codes of practice. However, it would be useful to also have a more active participation of industry associations and civil society bodies in activities such as promoting awareness among data fiduciaries of their obligations under this Act, promoting measures and undertaking research for innovation in the field of protection of personal data.

8. *The Authority must be empowered to exercise responsive regulation*

In a country like India, the challenge is to move rapidly from a state of little or no data protection law, and consequently an abysmal state of data privacy practices to a strong data protection regulation and a powerful regulator capable of enabling a state of robust data privacy practices. This requires a system of supportive mechanisms to the stakeholders in the data ecosystem, as well as systemic measures which enable the proactive detection of breaches. Further, keeping in mind the limited regulatory capacity in India, there is a need for the Authority to make use of different kinds of inexpensive and innovative strategies.

We recommend the following additional powers for the Authority to be clearly spelt out in the Bill —

i. **Informal Guidance:** It would be useful for the Authority to set up a mechanism on the lines of the Security and Exchange Board of India (SEBI)'s Informal Guidance Scheme, which enables regulated entities to approach the Authority for non-binding advice on the position of law. Given that this is the first omnibus data protection law in India, and there is very little jurisprudence on the subject from India, it would be extremely useful for regulated entities to get guidance from the regulator.

ii. **Power to name and shame:** When a DPA makes public the names of organisations that have seriously contravened data protection legislation, this is a practice known as "naming and shaming." The UK ICO and other DPAs recognise the power of publicity, as evidenced by their willingness to co-operate with the media. The ICO does not simply post monetary penalty notices (MPNs or fines) on its websites for journalists to find, but frequently issues press releases, briefs journalists and uses social media. The ICO's publicity statement on communicating enforcement activities states that the "ICO aims to get media coverage for enforcement activities."

iii. **Undertakings:** The UK ICO has also leveraged the threats of fines into an alternative enforcement mechanism seeking contractual undertakings from data controllers to take certain remedial steps. Undertakings have significant advantages for the regulator. Since an undertaking is a more "co-operative"solution, it is less likely that a data controller will change it. An undertaking is simpler and easier to put in place. Furthermore, the Authority can put an undertaking in place quickly as opposed to legal proceedings which are longer.

9. *No clear roadmap for the implementation of the Bill*

The 2018 Bill had specified a roadmap for the different provisions of the Bill to come into effect from the date of the Act being notified.[17] It specifically stated the time period within which the Authority had to be established and the subsequent rules and regulations notified.

The present Bill does not specify any such blueprint; it does not provide any details on either when the Bill will be notified or the time period within within which the Authority shall be established and specific rules and regulations notified. Considering that 25 provisions have been deferred to rules that have to be framed by the Central Government and a further 19 provisions have been deferred to the regulations to be notified by the Authority the absence and/or delayed notification of such rules and regulations will impact the effective functioning of the Bill.

The absence of any sunrise or sunset provision may disincentivise political or industrial will to support or enforce the provisions of the Bill. An example of such a lack of political will was the establishment of the Cyber Appellate Tribunal. The tribunal was established in 2006 to redress cyber fraud. However, it was virtually a defunct body from 2011 onwards when the last chairperson retired. It was eventually merged with the Telecom Dispute Settlement and Appellate Tribunal in 2017.

We recommend that Bill clearly lays out a time period for the implementation of the different provisions of the Bill, especially a time frame for the establishment of the Authority. This is important to give full and effective effect to the right of privacy of the individual. It is also important to ensure that individuals have an effective mechanism to enforce the right and seek recourse in case of any breach of obligations by the data fiduciaries.

For offences, we suggest a system of mail boxing where provisions and punishments are enforced in a staggered manner, for a period till the fiduciaries are aligned with the provisions of the Act. The Authority must ensure that data principals and fiduciaries have sufficient awareness of the provisions of this Bill before bringing the provisions for punishment are brought into force. This will allow the data fiduciaries to align their practices with the provisions of this new legislation and the Authority will also have time to define and determine certain provisions that the Bill has left the Authority to define. Additionally enforcing penalties for offences initially must be in a staggered process, combined with provisions such as warnings, in order to allow first time and mistaken offenders from paying a high price. This will relieve the fear of smaller companies and startups who might fear processing data for the fear of paying penalties for offences.

10. *Lack of interoperability*

In its current form, a number of the provisions in the Bill will make it difficult for India's framework to be interoperable with other frameworks globally and in the region. For example, differences between the draft Bill and the GDPR can be found in the grounds for processing, data localization frameworks, the framework for cross border transfers, definitions of sensitive personal data, inclusion of the undefined category of 'critical data', and the roles of the authority and the central government.

11. *Legal Uncertainty*

In its current structure, there are a number of provisions in the Bill that, when implemented, run the risk of creating an environment of legal uncertainty. These include: lack of definition of critical data, lack of clarity in the interpretation of the terms 'harm' and 'significant harm', ability of the government to define further categories of sensitive personal data, inclusion of requirements for 'social media intermediaries', inclusion of 'non-personal data', framing of the requirements for data transfers, bar on processing of certain forms of biometric data as defined by the Central Government, the functioning between a consent manager and another data fiduciary, the inclusion of an AI sandbox and the definition of state. To ensure the greatest amount of protection of individual privacy rights and the protection of personal data while also enabling innovation, it is important that any data protection framework is structured and drafted in a way to provide as much legal certainty as possible.

Endnotes

1 (2017) 10 SCC 641 ("Puttaswamy I").

2 Clause 42(1) of the 2018 Bill states that "*Processing of personal data in the interests of the security of the State shall not be permitted unless it is authorised pursuant to a law, and is in accordance with the procedure established by such law, made by Parliament and is necessary for, and proportionate to such interests being achieved.*"

3 (2019) 1 SCC 1 ("Puttaswamy II")

4 *Puttaswamy I, supra,* para 180.

5 (1978) 1 SCC 248.

6 *Ibid* para 48.

7 Puttaswamy I *supra* para 180.

8 *State of W.B. v. Anwar Ali Sarkar*, 1952 SCR 284; *Satwant Singh Sawhney v A.P.O AIR* 1967 SC1836.

9 (2016)7 SCC 353.

10 Dvara Research "Initial Comments of Dvara Research dated 16 January 2020 on the Personal Data Protection Bill, 2019 introduced in Lok Sabha on 11 December 2019", January 2020, *https://www.dvara.com/blog/2020/01/17/our-initial-comments-on-the-personal-data-protection-bill-2019/* ("Dvara Research").

11 "A Data Sandbox for Your Company", Terrific Data, last accessed on January 31, 2019, *http://terrificdata.com/2016/12/02/3221/.*

12 *https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=48550*

13 *https://main.trai.gov.in/notifications/press-release/trai-releases-telecom-commercial-communication-customer-preference*

14 Clause 3(20) — "harm" includes (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (ii) financial loss or loss of property; (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of service,benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal.

15 Clause 3(38): "Significant harm' means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence, or irreversibility of the harm."

16 Alex Hern "Anonymised data can never be totally anonymous, says study", July 23, 2019 *https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds*.

17 Clause 97 of the 2018 Bill states*"(1) For the purposes of this Chapter, the term 'notified date' refers to the date notified by the Central Government under sub-section (3) of section 1. (2)The notified date shall be any date within twelve months from the date of enactment of this Act. (3)The following provisions shall come into force on the notified date-(a) Chapter X; (b) Section 107; and (c) Section 108. (4)The Central Government shall, no later than three months from the notified date establish the Authority. (5)The Authority shall, no later than twelve months from the notified date notify the grounds of processing of personal data in respect of the activities listed in sub-section (2) of section 17. (6)The Authority shall no, later than twelve months from the date notified date issue codes of practice on the following matters-(a) notice under section 8; (b) data quality under section 9; (c) storage limitation under section 10; (d) processing of personal data under Chapter III; (e) processing of sensitive personal data under Chapter IV; (f) security safeguards under section 31; (g) research purposes under section 45; (h) exercise of data principal rights under Chapter VI; (i) methods of de-identification and anonymisation; (j) transparency and accountability measures under Chapter VII. (7)Section 40 shall come into force on such date as is notified by the Central Government for the purpose of that section.(8)The remaining provision of the Act shall come into force eighteen months from the notified date."*