The Dialogue™
INFORM ENGAGE IDEATE

DEEPSTRAT
STRATEGY. POLICY. ACTION

PRELIMINARY ANALYSIS

REPORT OF JOINT PARLIAMENTARY COMMITTEE ON THE PDP BILL, 2019

Preliminary Analysis

Report of the Joint Parliamentary Committee (JPC) on the PDP Bill, 2019

Version 1.0[1]

26th December 2021

Authored by: Shefali Mehta[2]; Karthik Venkatesh[3]; Shruti Shreya[4], Pranav Bhaskar Tiwari[5], Saksham Malik[6]

Editor: Kazim Rizvi[7]

[1] *This is a preliminary explainer basis our initial analysis of the report. The document is a work in progress and shall evolve over the next few weeks with a deeper exploration of the significance of the key provisions. A subsequent draft with more detailed analysis shall be published soon.*

[2] Programme Manager, The Dialogue.

[3] Programme Manager, The Dialogue.

[4] Senior Research Associate, The Dialogue.

[5] Programme Manager, The Dialogue.

[6] Senior Research Associate, The Dialogue.

[7] Founding Director, The Dialogue

TABLE OF CONTENTS

1. Introduction

The Joint Parliamentary Committee **(JPC)** on the Personal Data Protection Bill, 2019, tabled its report in both houses of the Parliament. The Bill had a long journey from the 12th of December 2019, when it was introduced in Parliament, to the 16th of December 2021, after being thoroughly analysed by the JPC. The deliberation process undertaken by the Committee is highly commendable. It encompassed one of the most comprehensive consultations by a Parliamentary Committee, with stakeholders from all walks, ensuring diverse views and opinions. At the end of the process, the report published by the Committee has a total of Ninety-Three recommendations, which is indicative of how the Committee has combed over every aspect of the legislation in question.

Tabling of the JPC's report in the Parliament is a step towards operationalisation of privacy in India as well as towards enacting a data protection law. As we move in that direction, there are areas and aspects that require further deliberation, to ensure that we give the people of India a robust, effective and a comprehensive data protection law.

Towards that objective, this analysis document endeavours to delve into the key legal and policy provisions enumerated in the report, compare the changes envisioned in this report from the earlier Bill and to discern the significance of these changes while proposing implementable recommendations towards the operationalisation of a progressive and rights enabling data protection regime in India.

2. Change of Title, and Long Title of the Bill along with Objects and Reasons

A significant move that affects the entire narrative of the legislation is the change in the taxonomy of the Bill, from 'Personal Data Protection Bill, 2019' **(PDPB)** to the 'Data Protection Bill, 2021' **(DPB).** This change has effectively widened the scope of the Bill to govern both personal and non-personal data **(NPD).** The change is echoed in different provisions, but most importantly, in Clause 2, which elaborates upon the application of the Bill. The Clause now reads *'Applicable of Act to the processing of personal and non-personal data'* and includes specifically the processing of personal and non-personal data (including anonymised data). The term non-personal data has also been defined by the Committee. However, the definition is not nuanced to truly bring out the intricacies of non-personal data. It merely states that data other than personal data is non-personal data. The Committee has also included non-personal data breaches within the purview of the definition of 'data breach' as recommended.

A notable departure from the previous attempts of drafting the Indian data protection law has been the attempt to entrench the national security exception to the norm, i.e., privacy. The addition of the phrase *'to ensure the interest and security of the state'*, in the long title of the Draft Data Protection Bill, 2021 makes national security a key objective of the bill. This is a significant change as the long title serves as an internal aid for interpretation of the statute by the Court.

3. Definitional Changes

Some of the significant changes include providing the definition of key terms such as consent managers, non-personal data, and social media platforms, along with the inclusion of psychological harm within the definition of 'harms'.

Though additions to terms defined are welcome, there are certain areas that need further refinement. There is a need to elaborate and clarify the term 'psychological harm', to remove any ambiguity in the way it may be interpreted. In terms of defining non-personal data, the approach adopted has been exclusionary and the deployment of a negative definition does not account for the nuanced nature of non-personal data.

4. Implementation Timeline

A phased implementation timeline of two years has been proposed by the JPC, which is a progressive suggestion, in line with the global best practices. It shall allow small companies to learn to comply, and larger companies with the time to renegotiate global contracts and rearrange their cross-border supply chains.

Moreover, it shall enable the Data Protection Authority **(DPA)** to coordinate and work closely with the industry and other stakeholders to alleviate concerns and provide guidance, lay down the codes of practice, and sign Memorandum of Understanding (MoUs) with other sectoral regulators to prevent regulatory clashes, which is a positive way forward. However, it is important to note that the Committee has not included this recommendation in the text of the draft bill attached with the report.

5. Definition of Child and Treatment of Children under the Framework

The definition of a 'child' under the framework, which impacts their ability to give consent on the internet, has witnessed no change. Over the past two years, this issue has been extensively debated upon, with many believing that India must align with global best practices under which a child is defined as an individual below thirteen years of age.

Developed jurisdictions such as the United States of America's (US) Children's Online Privacy Protection Act **(COPPA**) and the European Union's General Data Protection Regulation **(GDPR)** follow the same age barrier of thirteen. However, the Committee has agreed to go ahead with the earlier definition of below eighteen years. This is likely to impact compliance around the collection of parental consent.

Seeking consent from parents for the activities of the kids on the internet with a broad stroke mandate creates excessive compliance, starting from setting up age verification mechanisms within the organisation to linking the account or activity of the kid with that of the parent and verifying the relationship. It remains to be seen how this will translate into practice.

Keeping the best interest of children in mind, the Draft Data Protection Bill, 2021 vide Clause 26(1)(g) empowered the DPA to categorise data fiduciaries who process data related to children as 'significant data fiduciary'.

6. Data Portability

The Draft Data Protection Bill, 2021 is proposed to uphold the rights of the data principal (citizens whose data has been collected), including their right to be forgotten, the right to data portability, and the rights to access, correction, and erasure. All data fiduciaries that deal with personal data must now establish means by which these rights can be translated.

However, the JPC in its report did not provide any guidance on how data portability will be implemented if the data fiduciary must seek the DPA's clearance on every data portability request. Moreover, the requirement of data portability will place undue obligations on data fiduciaries and could result in mandatory disclosure of confidential information. Therefore, we believe that the DPA should determine the validity of request denials, while being obligated to maintain confidentiality in making any such examination.

7. Non-Consensual Processing Provisions

The Draft Data Protection Bill, 2021 lays down the requirement of obtaining the consent of a data principal for the processing of their personal data. However, Clauses 12 to 14 speak about exemptions from this core principle. The JPC has not recommended any significant changes regarding the manner in which these exemptions to consent are granted.

Clause 12 that deals with exemptions provided to the State from consensual processing retains the overbroad language from the earlier draft that exempts the State from

collecting consent for purposes of *'performance of functions of the State authorized by law'*. This further elaborates on scenarios such as the provision of services or benefit to the data principal, issuance of any certification, licence or permit, compliance with orders, laws in force, medical emergencies, and disaster management. The Committee within this Clause has now suggested inclusion of compliance with orders of courts, tribunals and even quasi-judicial authorities. However, the language used in this Clause still remains overbroad and might allow the executive to exempt itself from the collection of consent for almost all functions or activities undertaken by it. It is imperative that these exemptions are looked at with more nuance, considering that the main aim of this framework is to create a regulation that promotes a consent-based architecture in the sphere of data and privacy regulation.

JPC makes a similar recommendation in Clause 13, to make an exemption for consent collection for purposes relating to employment. Clause 13 of the Bill deals with processing of personal data necessary for purposes related to employment. Highlighting the fact that the employer cannot be given complete freedom to process personal data of employees without consent for employment purposes, the Committee recommended that the processing should be allowed 'only if it is necessary or can reasonably be expected by the data principal'. This recommendation is crucial to prevent instances of data misuse by the employer; including sharing of this data with other entities for anti-competitive purposes.

Concerns from a competition angle primarily arise due to the possibility of competitors entering into wage fixing agreements. These refer to agreements between companies to

fix wage or employee benefit levels, or agreements to not compete with each other on salaries, benefits, or other terms of employment. On 31st July 2018, the Federal Trade Commission charged a company that provides therapist staffing services with unlawfully colluding to limit pay for therapists and inviting other competitors to do the same. If employers are provided free reign to process employment data, including sharing them with competitors, it may cause adverse effects on competition in the relevant labour markets. Considering these instances of anti-competitive conduct, it is important to ensure that processing of employment data is not done in an "unreasonable" way. To this end, the recommendation of the committee can help ensure healthy competition in labour markets. However, at the same time it is critical to ensure addition of greater precision to the Clause at the time of its implementation to ensure adequate level of accountability of the employer to this end.

Clause 14 that allows for non-consensual processing pursuant to be specified by future regulations has also seen some changes. The Committee recommends conditions to be taken into consideration while developing these regulations. The changes made here now include the legitimate interest of the data fiduciary. Further, it has also now expanded the sub-clause relating to mergers and acquisitions to include other similar corporate combinations or restructurings.

8. Data Protection Authority

8.1 Appointment and Selection Process

The DPA established under the Act will perform a critical role in the digital economy. The aspects of independence and technical capacity of the regulator are vital points to be

addressed. JPC in its report has taken a few steps in this direction, however, there is still work to be done to ensure that the DPA is truly and effectively independent. The addition of the Attorney General, central government appointees from Directors of the Indian Institute of Technology (IIT) and the Indian Institute of Management (IIM), and an independent expert appointed by the central government within the Selection Committee for DPA are welcome additions. However, the appointment process remains executive-heavy since there is no member from the Judiciary or the Parliament in the Selection Committee.

This could possibly raise questions on the independence of the DPA, where independence of regulator is a critical component for the Bill to achieve adequacy status with the EU, UK and the US for bilateral data transfer and data access treaties.

The Draft Data Protection Bill, 2021 also mentions that '*the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entities in a country or, an international organisation'* if they provide *'an adequate level of protection'* which is indicative of future negotiations on adequacy between India and other countries. Additionally, the powers of removal of members of the DPA continues to remain with the central government, another point of concern affecting the independence of the said authority.

8.2 Institutional Design

Another missed opportunity for the JPC has been on engaging on the organisational structure of the DPA. There is a need to create a tiered structure with zonal/state DPAs

to address the broad ambit of functions that the regulator will undertake. The report does not go into substantial detail on these topics. This is crucial considering the wide range of functions expected to be undertaken by the DPA and India's large demography. The said regulator has the authority to penalise both central and state governments. Therefore, in such a situation, there is a need to reconsider the centralised structure of the DPA, and provide adequate representation to the states, in line with principles of federalism and separation of powers as envisaged under the Constitution of India.

Many Indian regulators adopt an institutional design that allows for participation at the state level, for example, the Consumer Protection Commissions, Human Rights Commissions, and the Information Commissions under the Right to Information **(RTI)** Act. The absence of tapping into India's federal governmental structure while viewing the institutional design of the DPA is likely to be felt during the implementation phase of the data protection legislation.

8.3 Functional Independence

Though the scope of the functions of the DPA has widened with the inclusion of non-personal data regulation, overall powers of the DPA have been diluted, especially in terms of its autonomy. Firstly, pertaining to the DPA's role in transfer of sensitive personal data outside India, its power to allow such transfers pursuant to contract or intra schemes has been diluted as per the JPC's recommendations. It is now required to consult with the central government while granting such approvals. Secondly, pertaining to the extent to which the orders of the central government are binding on the DPA, the JPC has now recommended extending this from merely questions of policy to all aspects of the

framework. This is likely to significantly impact the independence of the DPA. The powers of the central government have expanded much more significantly in comparison to the DPA in the appended bill.

8.4 Potential jurisdictional conflicts between other regulators and the DPA

Coordination between DPA and other regulators like the Competition Commission of India **(CCI),** Security and Exchange Board of India **(SEBI),** Reserve Bank of India **(RBI),** etc. can prevent regulatory burden and uncertainty for stakeholders within the digital ecosystem. However, the JPC has not rendered any recommendations pertaining to the same. Though, the Draft Data Protection Bill, 2021, seeks to resolve this by mandating that in case of jurisdictional overlaps, the DPA shall consult the relevant authority before taking any action, and the two authorities may even enter a Memorandum of Understanding **(MOU)** for coordinated action. However, clarity on such interactions and MOUs is still required.

It is encouraging to see the report reinforce collaborative approach by extending its scope to include 'economic activities' of the DPA. We hope that in the foreseeable future; this resolve is strengthened by guidelines on timelines and procedures for these consultations and MOUs.

To formulate these guidelines, a transparent approach that engages various stakeholders, including technology companies, government agencies and civil society, can prove to be extremely fruitful.

8.5 Protection of commercially sensitive information during investigations before the DPA

Protection of commercially sensitive information submitted during investigations and inquiries is an important aspect. Considering that India currently does not have a trade secrets law, it becomes especially imperative that relevant safeguards for data fiduciaries are in place. Clause 49(3) of the Draft Data Protection Bill, 2021, provides that the DPA shall not disclose any confidential information that is treated confidential by the fiduciary; except where the DPA is required to do so under any law or to carry out its functions. Considering the gravity of this concern, it was expected that the JPC would mandate the DPA to form regulations aimed at formation of confidentiality rings.

However, the same has not been done. We hope that either separate rule that pertain to the maintenance of confidentiality are formulated in due time, or the general rules on the functioning of DPA focus on this aspect, consequently, providing a robust confidentiality regime.

9. Cross Border Data Flows

The data localisation requirement has remained unchanged in the new draft, and it continues to be sought out as a solution towards protection of personal data, sovereign interests, and to allow simpler access to data for law enforcement. The critical personal data is still not defined, and the compliance uncertainty that this brings could affect the industry adversely. It may impact India's trade positions and commercial interests with the EU, US, UK etc. and cause hurdles in establishing data-transfer agreements and multilateral treaty arrangements. Most importantly, the provision in the Bill is drafted to

include adherence to localisation with retrospective effects. The recommendation reads, *"concrete steps must be taken by the Central Government to ensure that a mirror copy of the sensitive and critical personal data which is already in possession of the foreign entities be mandatorily brought to India in a time-bound manner."*

Moreover, there are certain aspects that require attention, as per the report, cross border data transfers are restricted in the event that they go against *'public policy'* or *'state policy'*. The usage of such broad terminology, in the absence of tight definitions or interpretations might add to uncertainty during implementation. Additionally, with respect to the sanctioning of transfer of sensitive personal data pursuant to contract or intra scheme changes, now mandate that the DPA must consult with the central government while giving such approvals. It is noteworthy that the localisation provisions in the 2019 version of Bill were less restrictive than those suggested by the Sri Krishna Committee.

The JPC also missed out on engaging on global data flow arrangements. There are multiple instruments through which data flows can be facilitated between countries which have enacted data protection laws. Through such instruments, countries can facilitate transfer of data between each other, while maintaining a high standard of privacy, which can be agreed upon as part of a bilateral or a multilateral treaty.

It is crucial that the data protection law is interoperable with global ecosystems. However, the JPC did not delve into this aspect, and the recommendations do not provide an outline into how the Indian data protection framework could incorporate interoperability and is harmonised with global data protection ecosystems.

The emphasis remains on data sovereignty, which while valid, does not alleviate concerns of industry and investors that look at India as a lucrative investment destination. Increased compliance and establishment costs for SMEs and start-ups is another major concern, which if not tackled effectively, might force existing players to exit and serve as an entry barrier for new enterprises and start-ups.

The technology world has also moved towards creating solutions that aid the protection of sensitive or confidential data during the processing cycle, for example, through methods such as confidential computing. Confidential computing refers to technology used in cloud computing that helps to isolate or segregate sensitive data during processing by ensuring it remains encrypted during that process. This is one example among many privacy enhancing techniques being employed during the life cycle of data from collection to processing that seeks to protect sensitive data from being vulnerable. However, the Committee has not delved into such technologies and its potential while viewing sensitive personal and critical personal data from a security lens and has instead preferred localisation as a solution.

10. Hardware Regulation

In another significant move, the report includes a new sub-clause 49 (2) (o) to regulate hardware manufacturers, which collect data from digital devices. As India moves towards the enactment of its first data protection framework, it is crucial to ensure phased operationalisation of measures covering different aspects of data security.

Targeted regulation of the digital ecosystem is paramount to build a safe and secure digital space. It must be noted that hardware manufacturers already seek certifications

from various sectoral regulators like the Bureau of Indian Standards (BIS), the Ministry of Electronics and Information Technology **(MeitY),** the Telecommunication Engineering Center **(TEC),** and the Wireless Planning & Coordination, among others. Moreover, Telecom Service Providers are mandatorily required to connecting their networks on devices that are designated as 'trusted products' from 'trusted sources', as envisaged under the National Security Directive on Telecommunication Sector. Bringing in device regulation within the purview of the data protection law, where the DPA will be required to monitor, test and certify hardware devices, might lead to regulatory overlaps with other sectoral regulators.

Accordingly, appropriate standards must be prescribed keeping all concerns and appropriate safeguards in mind including:

- Consulting with technical and industry experts; and
- Ensuing conformance with global testing and compliance standards to secure both informational privacy and ease of doing business.

11. Government Exemptions

No changes have been observed in Clause 35 of the Bill, which grants exemptions to the State from the applicability of the Bill. The government collects vital data from all citizens and is one of the biggest data fiduciaries, and any exemption granted must be narrowly constructed. It is indeed a positive sign that the inclusion of the term *"just, fair, reasonable and proportionate" r*elating to the procedure thus employed, have been included.

However, it would have also been helpful had the Committee narrowed the scope of the provision of such exemptions by listing out specific instances or purposes to reduce the potential for misuse of such exemptions.

Clause 35 of the Draft Data Protection Bill, 2021 retains the *'necessary or expedient'* standard for curtailment of civil liberties even when the *Puttaswamy judgement* explicitly mandates *'necessary and proportional'* standard as was envisaged in the Justice BN Srikrishna's report and the Personal Data Protection Bill, 2018.

This could lead to curtailment of civil liberties on the ground of 'expedience' without establishing that the curtailment is 'necessary and proportional' to the harm. It is pertinent to note that the Supreme Court has specifically outlawed 'expedience' as a standard and mandated 'necessity' in the *Rangarajan judgement*.

Further, the mandate for the State to follow a procedure which is just, fair, reasonable and proportionate does not fulfil the mandate in the *Puttaswamy judgement*, as the 'just, fair, reasonable and proportionate' is only a procedural guarantee and not a substantive touchstone for the State to invoke exemption under Clause 35. The State can invoke exception under clause 35 by simply showing necessity or expediency and need not demonstrate the necessity and proportionality as mandated in the *Puttaswamy judgement*. To ensure actual accountability and check on State power, it is crucial that instances or purposes for which such exemptions may be granted are explicitly laid down.

12. Inclusion of Non-Personal Data

By bringing in NPD within the ambit of the Draft Data Protection Bill, 2021, the JPC has effectively included the entire universe of data within the purview of its regulation. This has widened the regulatory perimeter to such an extent that there is less clarity on how the regulator will effectively regulate, how companies will comply, and how individuals will exercise the rights granted to them. It is pertinent to note that in many other advanced jurisdictions with established data protection regimes, personal data protection is treated entirely separate from non-personal data regulation.

While inclusion of non-personal data into the definition of breach has been suggested, the modalities through which this will be operationalised is still not precise and is bound to cause inordinate confusion and compliance overheads. Moreover, the procedure for access to non-personal data for public policy purposes to the government must be clearly defined. Right now, it allows the government to ask for `any data from any data fiduciary', making it rather broad.

This creates multiple sticking points for implementation and compliance. Firstly, without a clear indication of what can be personal and non-personal data- data classification at the back end of the business becomes tricky. Especially for global businesses that are to comply with provisions of multiple regulations, a very broad mandate without adequate guidance will make it harder to comply, even though the intent is aligned with compliance. Moreover, implementing provisions that relate to non-personal data might be tougher at the moment, given the lack of know-how and insight into the manner in

which companies are operating. It might be prudent to engage in widespread consultation with stakeholders before such a provision is finalised in the text of the Bill.

The purpose and genesis of the Draft Data Protection Bill, 2021 is to protect the informational privacy of individuals whereas the requirement to regulate NPD stems from the objective to unlock economic value of data to benefit citizens, businesses, and communities in India. Given these divergent purposes, housing the regulation of both sets of data under the umbrella of one legislation would not achieve the latter purpose.

12.1 No clarity on the proposed regulation of NPD

The JPC report includes only certain amendments on NPD across the Draft Data Protection Bill, 2021, which includes 'non-personal data breach' and 'reporting obligations', while other aspects of data protection continue to apply exclusively to personal data. This demonstrates a lack of clarity on the way NPD is supposed to be regulated in the new version of the Bill. We believe that the inclusion of NPD to the Bill, 2021, without the full assessment of its impact, applicability, and purpose, would create ambiguity and conflicts within the new law.

12.2 Intellectual Property Rights Conflicts

It is unclear how the Government will regulate the use of anonymized data. Given that NPD would potentially encompass all information that a company deals with, any excessive regulation of the same may violate intellectual property rights that companies may have over certain aspects of this information.

12.3 Regulation of NPD by the DPA

The GDPR is recognized as the most significant regulation on privacy and data protection so far. According to the GDPR, data protection principles must only apply to such information concerning and identified or identifiable natural person, and therefore may not apply to such information that does not relate to any identifiable person. Therefore, anonymised data may be kept outside the purview of the Bill.

The DPA ideally may prescribe standards for anonymisation, and penalties for unauthorized de-anonymization to regulate the applicability of the Data Protection Law.

13. Platform Regulation & Intermediary Liability

13.1 Treating Social Media Platforms as Publishers

While the Draft Data Protection Bill, 2021 does not contain any provision regarding treating social media intermediaries as publishers, the JPC report contains a recommendation to this effect. The report proposes that digital platforms acting as intermediaries should be construed as publishers of the content hosted on their platform. This recommendation stems from the view regarding the intermediaries exercising control over the access to content hosted by them. Transparency and accountability in the platform's actions are critical for building a robust platform regulation framework. However, this recommendation is inconsistent with the established principles of intermediary liability as propounded in *Shreya Singhal judgement.*

The attempt to regulate social media entities is beyond the purview of this Bill, whose objective is to formulate a robust data protection framework. The proposal runs contrary to the established principles of platform regulation as envisaged under the Information Technology (IT) Act and its ensuing Rules, which is the primary framework for the regulation of social media. The IT Act accords 'safe harbour' protection to intermediaries under which they are provided immunity from liability in respect of user-generated content in absence of 'actual knowledge' regarding its illegality.

Taking away this protection might lead to self-censorship by the intermediaries causing a disproportionate impact on the right to online free speech of the citizenry.

13.2. User Verification

The recommendation advocates for mandatory verification of social media accounts as an essential requirement for social media platforms to enjoy their intermediary status. This would undermine the principle of data minimisation as it would increase the amount of personal data held by social media platforms. There is indeed a legitimate need to tackle online safety threats which have been increasing tremendously due to the proliferation of bots and fake accounts. However, the dire impact of this recommendation on the right to anonymity which empowers users with their privacy and free speech also cannot be negated. Anonymity serves to keep the free flow of information and opinions in a digital space. The mandatory verification can also adversely affect journalists, human rights workers, LGBTQ+ groups and other communities who resort to anonymous identities on social media to share their opinion.

13.3. The single regulatory body for online and print media

Moreover, the recommendation regarding the constitution of a single statutory body to regulate content published in print media as well as on social media platforms is an infeasible measure. Undeniably, appropriate regulation of the media space is critical to ensure the integrity of the published content, however, a *one size fits all approach* is inappropriate. The social media platforms operate as a conduit wherein they only host or transmit third party user-generated content. The content hosted by these platforms is not created by them while print media is the actual publisher of the content that they host. Given the differential nature of their functioning, it is paramount to ensure targeted regulation of both entities in accordance with the specific demands of both sectors.

14. Algorithmic Disclosure

Algorithmic disclosure as envisaged in Clause 23 (1) (h) of the Draft Data Protection Bill, 2021 is a change from the previous draft. Similar provisions have been envisaged in the EU's Digital Services Act and also in the Santa Clara Principles on Transparency and Accountability in Content Moderation 2.0.

The Draft Data Protection Bill, 2021 obligates the data fiduciary to ensure transparency in terms of fairness of the algorithms or methods used in the processing of personal data. Such disclosure empowers the data subject to understand the reasons behind the decision and to prevent discriminatory or otherwise legally non-compliant decisions by the data fiduciary. However, it is crucial to note that such requirements must not lead to forced disclosures of proprietary information and algorithms by data fiduciaries.

The wide ambit of this provision without clear delineation of the process and mechanism to order such a disclosure and the authority who would be entrusted with the power to issue such an order, poses concerns around its abuse owing to ambiguous wording. Moreover, the scope of such disclosure is also not defined, a lot has been left for subsequent regulation within the ambit of Clause 23. Public access to these algorithms may end up providing the bad actors with the tools to sidestep the algorithms and misuse the platform. Instead of mandating disclosures, it would be ideal to recommend strict standards and thresholds to assess the 'fairness' of such algorithms or methods deployed by data fiduciaries. Moreover, it is important to engage in stakeholder consultations and assess the industry practises best suited for India before mandating algorithmic disclosure under the Bill.

15. Penalties

The penalties that are prescribed in the Bill continue to include criminal penalties for re-identification, financial penalties, and the possibility of instituting class action suits in case multiple persons suffer from privacy violations from the same data fiduciary.

Penalties calculated by using either a limit or a percentage of annual turnover are progressive measures. The criminal liability clauses however, especially jail terms, are still seen as a strong deterrent for many start-ups and Small and Medium Enterprises (SMEs) from innovating. The criminal penalties that are prescribed in the Bill are severe, with prison terms of up to three years for matters related to careless dealing with personal data. In order to adhere to principles of proportionality, and to incentivize innovators and entrepreneurs, every effort must be taken to do away with criminal liabilities.

This page has been left blank intentionally.

About the authors

Shefali Mehta
Programme Manager, The Dialogue

Karthik Venkatesh
Programme Manager, The Dialogue

Shruti Shreya
Senior Research Associate, The Dialogue

Pranav Bhaskar Tiwari
Programme Manager, The Dialogue

Saksham Malik
Senior Research Associate, The Dialogue

The Dialogue
www.thedialogue.co

DeepStrat
www.deepstrat.in

Recommended Citation: Shefali M., et. al., (December 2021), Preliminary Analysis: Report of The Joint Parliamentary Committee (JPC) On The PDP Bill, 2019, New Delhi, The Dialogue and DeepStrat.

About the organisations

The Dialogue
Recognised as one of the top 10 think tanks to be watched out for by the University of Pennsylvania.
The Dialogue works on the intersection of technology, society and public-policy.

DeepStrat
DeepStrat is the leading authority on risk management & mitigation, public policy, geo-political risk and conflict resolution. DeepStrat was founded by a group that includes those who served in the top echelons of the Indian government in fields as diverse as intelligence, policing, military and international relations. Its founding members also include experienced public policy, legal and media professionals who served in leadership roles for decades. DeepStrat facilitates different stakeholders to come together and resolve contentious issues backed-by cutting edge research.