Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Analysis of the Data Protection Bill, 2021: Social media regulation and powers of the Government

Akhil Surya[a]

[a]NALSAR University of Law, Hyderabad, India

Received 24 December 2021; *Accepted* 05 January 2022; *Published* 08 January 2022

Growing awareness about the right to privacy in personal data, and the implications of an unregulated data ecosystem can have on national security and the economy create a strong need for legislation on data protection. The Personal Data Protection Bill, 2019 precisely serves this purpose by codifying the privacy rights of an individual, situations in which the Government can act overarchingly without individual consent, and obligations on entities collecting, storing, and transferring data. A Joint Parliamentary Committee was constituted to examine the bill and come up with a new version after deliberations. The Committee has been around quite for some time having conducted around 70+ sittings and 140+ hours of discussions. This article shall analyse the important and controversial clauses and features in the draft report presented by the Committee. It shall outline certain key features that were introduced newly in the draft report. The article, however, shall not deal with the entire multitude of clauses under the bill. Then, an exacting analysis is brought in regarding social media regulation and the government's unbridled power under the bill. The analysis is based on the core of a personal data protection bill: an individual's right to privacy. The Committee has failed to utilise the opportunity to fill the lacunae in the existing bill and further diluted the bill with regards to the government's power. It is high time that the Parliament shall carefully discuss the clauses beginning with some fundamental questions about the right sought to be protected, entities sought to be regulated, and exemptions it seeks to grant.

Keywords: *data protection, right to privacy, data legislation, social media regulation, surveillance programs.*

INTRODUCTION

In a world of interconnected technologies and communications proliferating rapidly, data is a vital source for new-age economies and innovations. Today, data exists as an asset for many corporations and governments for providing personalized services and designing interactive technologies.[1] Its importance brings with it constant threats against individual privacy, national security, and economic development. Data, though an intangible asset, does not exist independently from a physical presence in things, persons, or places. Personal data breaches have become a common phenomenon in the digital landscape posing threats not only to the individual's privacy but also to the interests of the territorial state.[2]

Naturally, individual data privacy concerns have forayed into states' regulatory frameworks in the recent past. Today, there are more than 120 states around the world that have different legislations in force to regulate data privacy, internet speech, and the collection and storage of data by giant corporations.[3] It was not until 2018 that the General Data Protection Regulation (GDPR) broke the ground as the most comprehensive legal instrument regarding personal data and its security.[4] This article shall not deal with the entire international landscape in this regard. It rather concerns itself primarily with India's recent Joint Parliamentary Committee (JPC) draft report on the Personal Data Protection Bill, 2019 (PDPB). It shall go on to highlight the importance of data privacy and locate certain controversial aspects of the draft report in the overall regulatory framework.

---

[1] Kean Birch, DT Cochrane & Callum Ward, 'Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech'(*Sage Journal,* 16 May 2021) <http://dx.doi.org/10.1177/20539517211017308> accessed 22 December 2021

[2] Michael Hill & Dan Swinhoe, 'The 15 biggest data breaches of the 21st century'(*CSO Online,* 16 July 2021) <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html> accessed 22 December 2021

[3]Andara Coos, 'Data Protection Legislation Around the World in 2021'(*Endpoint Protector,* 08 January 2021) <https://www.endpointprotector.com/blog/data-protection-legislation-around-the-world/> accessed 22 December 2021

[4] General Data Protection Regulation, 2016

THE EXISTING SETTING OF DATA PROTECTION IN INDIA

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Data Protection Rules")[5] notified under Section 43A of the Information Technology Act, 2000 ("IT Act")[6] currently is the only instrument governing data protection in India. Obtaining the consent of the individual before obtaining information, restrictions on the transfer of data, and publishing a uniform privacy policy with a grievance officer are some essential features of the Rules. These Rules apply to several social media platforms including Twitter, Facebook, and WhatsApp. Except for issuing secondary rules and regulations under sections of the IT Act, the Union Government has paid little regard to data protection legislation until 2017.

The discussion for data privacy legislation arose only in 2017, with the landmark judgement in the *K. Puttaswamy v Union of India* case, where privacy of an individual was held to be inherent in protected fundamental rights including the right to live with dignity and self-respect under Article 14, 19 and 21 of the Constitution.[7] The right to privacy obtaining its constitutional basis, the creation of GDPR, and surrounding threats to India's national security caused by its vulnerability in data protection have all cemented the need for legislation protecting individual's privacy from any unlawful interference without consent. In 2018, Justice B. N. Sri Krishna Committee submitted its report and proposed to enact a data protection law. The draft report was adopted by the Union Legislature and consequently, the PDPB was introduced. PDPB, while protecting the rights of the data principals (individuals), imposes obligations on data fiduciaries (entities collecting such data) and grants exemption to the Government in certain situations. The introduction of the bill, followed by an immediate uproar by the opposition members, civil society organizations, and experts led to the creation of a JPC to deliberate upon the clauses in the bill and make respective recommendations. Nearly 2 years

[5] Vinod Joseph, Protiti Basu & Ashwarya Bhargava, 'India: A Review Of The Information Technology Rules, 2011 Reasonable Security Practices And Procedures And Sensitive Personal Data Or Info'(*Mondaq*, 19 March 2020) <https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-> accessed 22 December 2021

[6] Information Technology Act, 2000

[7] *K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1

later, the JPC has released its report with an updated version of the bill titled "The Data Protection Bill, 2021".

KEY FEATURES OF THE DRAFT REPORT

1. The draft report expands the very subject matter of the bill. The PDPB, initially seeking to protect and regulate personal data, is now recommended to include non-personal data within the same bill. Two points must be articulated at this juncture. First, the fundamental right to privacy applies to data in as much as it is considered to be personal, thus, non-personal data is largely outside the ambit of the *raison d'etre*of the initial bill. Second, by virtue of clause 92 in the report, the bill now grants unqualified powers to the Union Government to make "*any* policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, and handling of non-personal data". To further complicate matters, clause 92 is the only concrete provision regarding non-personal data with no checks whatsoever.

2. The Data Protection Authority, the apex body of institutional architecture, was initially proposed to be an independent regulator. According to the JPC draft, the DPA shall now contain a chairperson and not more than 6 persons nominated directly by the Union Government. Countries with similar authority under a data protection law have clauses requiring fair competition in nominating members. The extensive control of the Union Government in appointing the authority at its own will without consulting the Parliament is concerning and fundamentally different from the initial bill.

3. Mandatory reporting by data fiduciaries to the authority within a 72-hour period in case of a data breach is a commendable recommendation made in the draft report as it gives concrete effect to the provision.[8] Tilt in favour of a protectionist data localisation is another significant feature in the report. It has been equally criticised and appreciated given its effects on the

[8] Data Protection Bill, 2021, s 25

interests of the State and entities which need to comply with these requirements.[9] The recommendation to set up an official certification system for all the digital devices ensuring integrity to strengthen data security is another novel feature introduced in the draft report.[10]

A DETAILED ANALYSIS

Broadly, three stakeholders can be identified in all versions of the bill commonly: individuals (data principal), companies and corporations (data fiduciaries), and the State. Individuals' right to privacy ought to be protected both from private and state interference. Similarly, the State ought to regulate data fiduciaries in the best interests of both the parties and they shall comply. The draft report confuses these seemingly simple presumptions. In defence of the draft report, it can be stated that given the complex nature of the technology and associated sectoral requirements in the digital economy, the draft report is comprehensive and must not be examined strictly where there exists a complete vacuum of law in this regard, and the system must be given some time to see how the regulatory mechanism might play out.[11] Though there exists plausible merit in the argument, the answer to the question of why a bill drafted to protect an individual's right to privacy in data does more to the State than it does for the individual remains elusive. Further analysis is based on this fundamental argument and is divided into two sections discussing the most contentious issues.

REGULATION OF SOCIAL MEDIA

Uninhibited access to the internet and uncontrolled space to express one's views and beliefs needs no further explanation. Access to the internet and the fundamental right to free expression of speech have been founded firmly in the Indian Constitution in the Anuradha

[9] Trishee Goyal, 'Personal Data Protection Bill: 4 Reasons Why Governments Bat for Data Localisation'(*News18,* 06 December 2021) <https://www.news18.com/news/opinion/personal-data-protection-bill-4-reasons-why-governments-bat-for-data-localisation-4525034.html> accessed 22 December 2021

[10] Sneha Rao, 'Personal Data Protection Bill : What Does Joint Parliamentary Committee Report Say?' (*Livelaw,* 20 December 2021) <https://www.livelaw.in/top-stories/data-protection-bill-report-joint-parliamentary-committee-exemptions-non-personal-data-childrens-data-right-to-privacy-188048> accessed 22 December 2021

[11] Kaveri Chandrasekhar, 'Is India ready for the regulation of Non-Personal Data under the Personal Data Protection Bill, 2019?'(*Yourstory,* 02 November 2021) <https://yourstory.com/2021/11/non-personal-data-regulation-under-personal-data-protection-bill-2019/amp> accessed 22 December 2021

Bhasin judgement.[12] Speech on such social media platforms is predominantly governed by community guidelines or the policy of the said application. The proliferation of fake accounts and bots which can post content on any social media space is worrisome, and interestingly, finds detailed mention in the draft report. The uncontrolled access to post any types of defamatory or seditious content on social media poses a great challenge to the State to enable themselves to effectively regulate content and take enforcement measures.[13]

At this juncture, it is important to understand the difference between a "social media intermediary" and a "social media platform". Though the terms are commonly used interchangeably, they have significant meaning and effect. According to the IT Act, a social media intermediary is one that merely hosts users to post, share or store content without having any control over the content. Major social media applications like Facebook and Twitter have the status of "social media intermediary" meaning that these companies cannot be held liable for any unlawful or objectionable content posted on their interface. Rather, the user or individual who posted the content shall be held liable in case of any breach of law with the content posted. Having deliberated on the threats posed by fake accounts and botnets, the Committee seems to have taken the approach to hold the social media company instead, thus, making them a "social media platform" by definition. Social media platforms essentially are similar to original publishers as newspapers, magazines, and films where the newspaper editor or film company has sole authority over the content they post or publish. In any case, the content is found to be unlawful, it is the newspaper or film-maker that is held directly liable. The Committee, in para 1.15.12, stresses the "immediate need for regulation" and believes that the IT Act "has not been able to keep pace with the changing nature of the social media ecosystem". The draft report cumulatively states that the status of intermediary is not suited to these social media applications because they have sufficient control to bring down any content or restrict sharing. The draft report makes sweeping changes in the bill by replacing "social media intermediary" (as provided in PDPB, 2019) with "social media

[12] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637

[13] Shweta Venkatesan, 'Parliamentary Committee's PDP Bill report isn't enough. Social media liability needs better' (*The Print,* 04 December 2021) <https://theprint.in/opinion/parliamentary-committees-pdp-bill-report-a-low-hanging-fruit-data-privacy-needs-rethink/776015/> accessed 22 December 2021

platform" in every single iteration and adventurously goes on to suggest that a statutory media regulatory authority like the Press Council of India be set up.

Clause 26 and clause 28 of the bill must be examined to reach a conclusive remark in this regard. Irrespective of what the employed phrase from the two will be, these social media giants house and often transfer across India a humongous volume of personal data. As already mentioned, an entity engaging in storing, collecting, and transfer of data is called a "data fiduciary" under the bill. Clause 26 allows the Authority to notify any data fiduciary as a "significant data fiduciary" by taking into consideration several factors laid down within the section. Social media platforms (as amended) are further necessitated to enable verification of users voluntarily under clause 28 indicating the explicit intent to *regulate* social media and content therein. Though the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[14] issued under the IT Act addresses the accountability issue of content posted, they are the subject matter of severe criticism and pending litigation in courts across the nation. A tussle well-known to the public between the Union and Twitter over non-compliance with such requirements raises further concerns.

Firstly, the Committee misses a simple difference in making an analogy with original publishers like newspapers with social media. Unlike a newspaper, a social media company can only bring down or delete content and not approve each post a user wishes to post. Thus, in no event, a social media application can be held to be a social media platform according to the definition. Secondly, an attempt to address the accountability issue in the current legislation prima facie seems far-fetching. Giving final discretion to the social media platform over content curbs users' freedom of speech indefinitely and confuses users as to what content is permissible in the absence of a clear policy by the platform.

The purpose and scope of the bill are not to be forgotten in the larger fiasco of social media regulation. Social media regulation outrightly falls outside the scope of the bill. Resorting to PDPB as a forum to deal with social media regulation, which was not possible with an

[14] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

extensive IT Act is not logically plausible either. Even considering the merits of the framework the Committee advocates for, the effects go against the desired object. The freedom social media grants cannot be curtailed as this goes against the fundamental rights of the individuals. This also imposes an unfair burden of compliance costs on social media companies. Therefore, the draft report does no good for an object it seeks to found on a bill that does not even allow for any matter in this regard. If India ought to regulate social media in the interests of the State, the PDPB is not the space to do so. Rather, following the approach taken by UK and Singapore[15], the Union shall venture into social media regulation under defamation, sedition, and communication laws.

OVERARCHING POWERS OF THE UNION GOVERNMENT

All fundamental rights protected by the Indian Constitution including Article 21 are not absolute in nature. Fundamental rights in effect exist in constant tension between the protected nature of the rights held by an individual and the paramount interests of the State.[16] This analysis shall not delve into the scrutiny of constitutional standards of clauses restricting the rights of individuals in the draft report or the bill. It is, nevertheless, important to bear in mind the inherent but limited power of the state to curtail fundamental rights. Individuals' right to privacy in data, emanating from Articles 14, 19, and 21 thus cannot exist free from any restriction by the state. However, the restrictions or any interference by the State in fundamental rights including the right to privacy must be non-arbitrary, reasonable, and lawful. The further analysis, in three separate heads, shall be based on the changes the draft report makes in the powers of the Union, the right sought to be protected, and serious proximity of misuse.

- **Clause 35 under Exemptions:**

[15] Apar Gupta, 'National security, at the cost of citizens' privacy'(*The Indian Express,* 20 December 2021) <https://indianexpress.com/article/opinion/columns/national-security-at-the-cost-of-citizens-privacy-7680787/> accessed 22 December 2021

[16] *Maneka Gandhi v Union of India* (1978) 1 SCC 248

The most notable, yet controversial, clause 35 has been the subject of gradual dilution throughout the lifetime of the law. Clause 35 allows the Union Government to exempt any agency of government from any or all provisions of the bill. The 2018 draft presented by Justice B.N. Sri Krishna Committee circumvented this wide exemption clause with necessity, legality, and proportionality. The first change in 2019 has omitted proportionality and legality and replaced them with "necessity" and "expediency". The emphasis on expediency and not legality has drawn criticism from Justice Sri Krishna himself calling out the shift in the clause as leading to an "Orwellian state" and a "dangerous trend".[17] The draft report, further, adds more to the woes against wide power conferred to the Union.

Firstly, the non-obstante clause must be understood. The draft report recommends the clause, to begin with, the words "notwithstanding anything contained in law for the time being in force" meaning that the clause shall have primacy not only over the bill in discussion but also any other law in force. Secondly, public order has been provided to be ground under the clause. Public order in Indian law has a very wide ambit extending from the security of the state to public tranquillity and peace. The explicit mention of "incitement of any cognisable offence" further dilutes the threshold to be met under the clause. A cognisable offence under the Indian criminal law spans from simple murder to preparation to wage a war against the state. The phrases used under clause 35 give almost absolute power to the Union Government to act at its whim. Undeterred by several dissent notes from the likes of Shri Jairam Ramesh to omit public order as a ground, the Committee has proceeded with the same clause.

Thirdly, the Committee seems to assume that it has taken a noble step by explaining the words "such procedure" in the clause. The words, when located in text and effect of the clause, have no actual bearing. The Union Government shall only follow a fair and reasonable procedure in passing the order recording reasons to exempt the agency and not the substantial standard for granting the exemption. In effect, the Union Government can still continue to grant exemption

[17] MeghaMandavia, 'Personal Data Protection Bill can turn India into 'Orwellian State': Justice BN Srikrishna'(*The Economics Times,* 12 December 2019) <https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice bnsrikrishna/articleshow/72483355.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> accessed 22 December 2021

to any agency under the wide and low threshold grounds. Fundamental rights are protected from interference by both, private and state actors. The draft report seems to have missed the essential premise herein granting the Government power to exempt its own agencies from its law protecting the rights of individuals. As a matter of preliminary conclusion, the draft report does not protect these rights against the State and only does so for private parties.

- **Surveillance programs:**

Surveillance programs conducted by the state on its citizens are a common phenomenon around the world amounting to a serious breach of individual's privacy when conducted unreasonably. The Committee seems to have been concerned with surveillance by foreign states while examining clauses relating to data localisation but evidently has forgotten surveillance by the Indian Government itself.[18] Today, there exist several intelligence and surveillance programs publicly known in India like Crime and Criminal Tracking Network and Systems (CCTNS) and National Intelligence Grid (Nat Grid).[19] Neither the draft report nor the bill mentions anything about the state's surveillance programs. Though such programs are necessary for swift enforcement measures among other reasons, they cannot be left out in legislation concerned with data protection and privacy. The draft report leaves the individual's right at peril and grants the Union a blank cheque once again.

- **Control over DPA**

As already discussed, the Union Government has complete authority over appointments to the Authority putting it under absolute satisfaction of the Union. Clause 86 (renumbered and as amended in the draft report) empowers the Central Government to issue any directions to the Authority on questions of policy and the Authority shall be bound by them. To make things worse, the draft report recommends that the words "on questions of policy" be omitted, rendering the directions, extending to any matter and not just policy, be fully binding on the

[18] Apoorva Mandhani, 'Non-personal data, social media — what new 'data protection bill' could look like'(*The Print*,06 December 2021) <https://theprint.in/theprint-essential/non-personal-data-social-media-what-new-data-protection-bill-could-look-like/776389/> accessed 22 December 2021

[19] Addison Litton, '*The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression*' (2015) 14 (4) Washington University Global Studies Law Review

Authority. A similar unqualified clause exists in clause 92 as already has been discussed. Overall, the Union Government can act at its own whim and effectively control the DPA defeating the whole purpose of a separate independent body to oversee the consistent application of the Act. The Union Government is not bound at least to take into consideration suggestions made in the Parliament or by the state governments meaning that the Central Executive has unbridled powers over the DPA.

CONCLUSION

The PDPB is the first legislation of its kind in India making it the centre of scrutiny and controversy. Different versions of the bill have been in the public domain for nearly four years now and a new concern emerges into the spotlight each time a change is made. The JPC has had a golden opportunity to settle concerns and ensure concrete application of the bill. Much to the dismay of the nation, the JPC has continued to ignore issues not addressed in the bill, cemented clauses that attracted severe backlash, and failed to clarify several provisions. Many changes were made at the last minute to the extent of expanding the long title of the bill to include "in the interests of the state".[20]

The draft bill proposed by the Committee now regulates social media platforms but the entire regulatory framework at odds with each other continues to allow the Government to be free from the obligation to interfere with the rights and limits the right only to certain entities and circumstances. In the whole process of deliberations and discussions, the gist of the bill: individual's right to privacy has lost its standing and shine. The JPC's work with the draft report is one of the most extensive ones in reconfiguring and re-examining legislation over a span of 70+ meetings making it sufficiently subject to criticism. The draft report is not binding on the Parliament to pass as proposed as it still reserves the report to discussion and passing. It is high time for the Union to ask itself some fundamental questions regarding the nature of the right, the scope of the bill, objects it seeks to achieve falling outside the scope of the bill, and its restricted role in the interference with the right to privacy.

[20] Data Protection Bill, 2021, s 1