VACILLATING BETWEEN NO LAW AND BAD LAW: AN ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

Huzaifa Shaikh[*] *and Dr. Radheshyam Prasad*[**]

ABSTRACT

In a bid to equip the country with a robust data protection system, the draft of the Digital Personal Data Protection (hereinafter, "DPDP") Bill was released by the Ministry of Electronics and Information Technology (hereinafter, "MeitY") on November 18, 2022. It is notable that this is not the first time the government has introduced such a legislation. The Data Protection Law has been in the pipeline for almost five years. There has been a lot of hue and cry about the previous Bill and it is apposite to say that the current Bill is also not free from any controversy. However, the key point to highlight is how these recommendations, revisions, and discourse surrounding the Bills proved to be of the essence for us, the people. The quest for a robust law and the unideal circumstances raise eyebrows regarding the intentions of the government and all the other stakeholders in

[*]Huzaifa Shaikh is a fourth-year B.A. LLB (Hons.) student. The author may be reached at huzaifahaider51@gmail.com.
[**]Dr. Radheshyam Prasad is an Associate Professor at the University of Lucknow. The author may be reached at radheshyampd@gmail.com.

implementing or trying to implement a regime focused on the individual's right to privacy as well as maintaining the sovereignty of a country's data.

The authors in the present article, while analyzing the anomalies of the latest DPDP Bill, 2022, compare its provisions with the standards going around the globe. In addition, reference is also made to the provisions of earlier Bills to comparatively analyse the contentious points. Besides, the authors also try to answer how a flawed data protection law would prove to be deadlier than no law. There is no doubt that a robust data protection law is the need of the hour, but the real challenge is, at what cost?

I. INTRODUCTION

The Central Government pulled back the Personal Data Protection (hereinafter, "PDP") Bill after a tight scrutiny by the Joint Parliamentary Committee,[1] which worked hard in determining key anomalies and proposing 81 amendments.[2] It is undeniably a regressive action for the Indian Government to choose to drop a crucial Bill after five years of labour rather than take into account the 81 amendments in the Bill. Therefore, the withdrawal makes it pertinent to analyze the key disputed provisions regarding data protection and also to see the

[1]'An Assessment of the JPC Report on PDP Bill, 2019' (*Economic and Political Weekly*, 31 July 2022) <https://www.epw.in/engage/article/assessment-jpc-report-pdp-bill-2019> accessed 2 January 2023.

[2]Maru, 'Why Personal Data Protection Bill 2019 Withdrawn in India?' (*TechHerald*, 4 August 2022) <https://techherald.in/news-analysis/why-personal-data-protection-bill-2019-withdrawn-in-india/> accessed 12 January 2023.

rationale behind such provisions in order to comprehend the question of whether the disputed provisions have really been scrapped or have just changed their clothes in the recent 'Digital Personal Data Protection *(*hereinafter, "DPDP") Bill'?

The ultimate bone of contention in the PDP Bill of 2021 had been the 'sweeping power' which was granted to the Government along with the unchecked control of the Data Protection Authority established under the said Bill. The incidental effect of the same was manifold as it not only facilitated arbitrariness, but also was in direct violation of the right to privacy. The right to privacy has been given recognition as a fundamental right vide the *K.S. Puttaswamy* case,[3] and the debate for a robust data protection law also emanated from the same.

India has long struggled to put forth a perfect and uncontroversial privacy law. The 'Information Technology Act of 2000' and IT Rules (2011),[4] which deals with technological and privacy issues are the current legal framework. These laws have not kept up with technological advancements and thus, a proper data protection law is becoming increasingly necessary, especially considering the *K.S. Puttaswamy* judgement mentioned above. Therefore, there is no question that India needs to enact a legislation that is flawless in terms of privacy and data protection. The data protection law has been in the pipeline for years and because of its importance, it was heavily debated and criticized. Many stakeholders have put in their efforts to strengthen the regulation. With multiple suggestions and criticism surrounding the contentious data protection Bill, the Union Government proposed the Bill to the Joint Parliamentary Committee (hereinafter, "JPC") for recommendations back in December 2021.[5] Even after receiving

[3] *Justice K S Puttaswamy & Anr v Union of India & Ors* (2017) 10 SCC 1.
[4] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
[5] Joint Committee on the Personal Data Protection Bill, 2019' (*PRS Legislative Research*, 5 March 2023) <https://prsindia.org/parliamentary-committees/joint-committee-on-the-personal-data-protection-bill-2019> accessed 25 November 2022.

detailed recommendations from the JPC, the government withdrew the Bill, which has not only attracted raised eyebrows but also has brought us to square one. The defense that a thorough legal framework, in light of the JPC's recommendations, is being brought up by the MeitY[6] did not seem promising.

Even after its introduction in the form of a comprehensive DPDP Bill, the majority of stakeholders seems unhappy and have chalked out various anomalies. *Per contra*, provided the constant opposition to the Bill from the multinational digital tech giants or 'big tech', supported by the United States government, it is entirely plausible that pressure from outside the nation caused the PDP Bill to be withdrawn, than to entertain recommendations.[7] Irrespective of the controversies, the pullback has led to the nullification of many years of efforts of various stakeholders in shaping the law. Coupled with this, the current legislation has various loopholes and serves no purpose with regards to the recommendations put forth by the JPC.

The authors, in the present article, first explore the intention of the legislature by analyzing the anomalies of the Bill. Secondly, a comparison has been drawn between the current provisions and that of the earlier draft and the recommendations of the JPC to the same. Thirdly, in light of the loopholes, the authors argue how flawed data protection legislation will be detrimental to the country. To substantiate the same, the authors rely on two crucial global examples *viz.* the *Cambridge Analytica* Case and access to data in the times of Covid 19 Pandemic. As the provisions of the DPDP Bill are also inspired by the

[6]'IT Ministry will soon come up with new version of Data Protection Bill, says Union Minister Ashwini Vaishnaw' (*ETCIO.com*, 6 September 2022) <https://cio.economictimes.indiatimes.com/news/big-data/it-ministry-will-soon-come-up-with-new-version-of-data-protection-bill-says-union-minister-ashwini-vaishnaw/94016121> accessed 4 February 2023.

[7]Barik S and Aryan A, 'US Bodies Push Back on Data Protection Bill, Seek New Working Group' (*The Indian Express*, 3 March 2022*)* <https://indianexpress.com/article/india/us-bodies-push-back-on-data-protection-bill-seek-new-working-group-7798193/> accessed 10 November 2022.

EU Regulations, the authors lastly analyze the common denominators of both the Regulations on certain parameters.

II. DEMYSTIFYING THE INTENTION OF THE LEGISLATURE

Although it is the job of the court to interpret the legislation when it actually comes into force and demystify the confusion with respect to the statute or any part thereof, the controversy pertaining to the Data Protection Law has done one good thing i.e., it has helped various stakeholders to chalk out various loopholes and look through the legislative intent. The PDP Bill of 2021 and the DPDP Bill of 2022 have been criticized for more than a few reasons. Some of the common contentious provisions which are worth highlighting are discussed below:

A. Blanket Protection Bill for exclusive control by the State

The key anomaly in the prior Bill was its Clause 35 as it attracted much controversy with regards to the *blanket protection* which is granted to government agencies by way of exemption provision enshrined in the same.[8] The provision departed significantly from what the panel headed by B.N. Srikrishna proposed in its initial draft in July 2018.[9] The same provision is exactly reflected in Clause 18(2)(a) of the DPDP Bill 2022. This provision again is in direct contrast to the initial draft which suggested that the data of an individual will not be processed by anyone *without free consent*. The draft also suggested that if there has to be any processing of data without consent, then it should be in

[8]Ajay Kumar Bisht and Dr. N. S. Sreenivasulu, 'Clause 35 of The Personal Data Protection Bill, 2019: Whether a Reasonable Restriction or a Withering Away of Fundamental Right to Information Privacy?' (2022) 5 (2) IJLMH.

[9]Saigal S, 'Data Protection Bill Not in Line with Draft: Justice Srikrishna' (*The Hindu*, 18 December 2019) <https://www.thehindu.com/news/national/data-protection-bill-not-in-line-with-draft/article61605540.ece> accessed 10 December 2022.

consonance with three principles i.e., the objective sought to be achieved, proportionality, and reasonability.[10] However, neither the current Bill nor the prior Bill laid down such abiding principles. By looking through the democratic lens, this provision paves no hurdle-free path and is clearly not in the interest of democracy.[11] Since government agencies are always presumed to remain in line with the State's duty to protect against breach of privacy of its citizens, the 2021 Bill by virtue of Clause 12(a) and the current Bill vide Clause 8(2) grants exclusive right to the State to process the data in a non-consensual manner. This further underpins the controversy with regards to the control by the State which is *prima facie* unfair, unjust and arbitrary use of power.

B. Precedence of Central Government over Data Protection Board: an attempt to dilute the right to privacy

The DPDP Bill is asymmetrical in a sense that there is a clear precedence of the Central Government over the Data Protection Board (a regulator that would take action to protect individuals' interests and prevent misuse of personal data). This precedence has the ability to hinder the independence of members constituting the body. It is notable that the independence of the members is a *sine qua non* for ensuring its impartial and independent functioning. The term 'as may be prescribed' has been used quite often across various Clauses in the Bill. Even with regards to the Data Protection Board's establishment, in Clause 19(2), which provides for strength, the Board's composition, selection process, removal, requirements of appointment and service, the determination of all these factors has been left to the term 'as may be prescribed'.[12] In legislative drafting, the term 'as may be prescribed'

[10]ibid.
[11]*I R Coelho v State of Tamil Nadu* (2007) 3 MLJ 423 (SC).
[12]Jain A, 'IFF's First Read of the Draft Digital Personal Data Protection Bill, 2022' (*Internet Freedom Foundation,* 19 November 2022) <https://internetfreedom.in/iffs-

is frequently used to delegate authority to regulatory bodies to create detailed regulations that support the broader objectives of the law.[13] While this approach offers adaptability, but at the same time, it also raises concerns about arbitrariness, particularly in contexts where transparency and accountability are paramount. The phrase 'as may be prescribed' has been mentioned 18 times for the 30 Clauses in the current Bill.[14] Thus, the inclusion of such terms in the legislation which is intended to regulate individual data could lead to varying interpretations of data protection standards thereby, potentially impacting individuals and businesses.

Furthermore, contrary to the diversified and independent composition proposed in the committee's draft, the Data Protection Board's makeup is dominated by the government. This is also dealt in length in the dissent notes that some JPC members attached to the report, in which they stated that if such power were not restrained by parliamentary supervision, it would result in a major weakening of the fundamental right to privacy.[15] Therefore, the existing structure of the statutory body is contrary to the objective of the law i.e., the members of the authority must be kept outside from the influence of any ruling government. Such an influence over a so-called independent body will not only have detrimental effects on the monumental right to privacy but it will also be contrary to the essence of the law. The Supreme Court in the case of *Mardia Chemicals v. Union of India*, very aptly held that, "*the real test to examine the essence of law is to view whether it provides*

first-read-of-the-draft-digital-personal-data-protection-bill-2022/> accessed 16 December 2022.

[13]*In Re: The Delhi Laws Act, 1912* AIR 1951 SC 332.

[14]Mathi B, 'Twelve Major Concerns with India's Data Protection Bill, 2022' (*MediaNama*, 1 December 2022) <https://www.medianama.com/2022/11/223-twelve-major-issues-data-protection-bill-2022/&gt> accessed 20 December 2022.

[15]Garg R, 'Dissent Is Democratic: Looking at the Dissent Notes in the Report of the JPC #Saveourprivacy' (*Internet Freedom Foundation*, 23 December 2021) <https://internetfreedom.in/pdpb-jpc-report-dissent-notes/> accessed 20 December 2022.

unreasonable and arbitrary power",[16] and remarkably by connecting the dots, i.e., the exemption to the government agencies vide Clause 18(2)(a) and the Central Government's control over the autonomy of Data Protection Board as provided under Clause 20(1)(b), the authors assert that the current Bill fails this test as well. Moreover, Clause 19(3) of DPDP Bill continues the same squabble of Clause 42 (2) of the 2021 Bill, wherein the chief executive of the board (earlier chairman of Data Protection Authority) is appointed by the government. As the Board (DPB) continues to lack the autonomy required to adequately protect Data Principals' interests, these provisions build on the shortcomings of its earlier incarnations.

C. Infringement of right to privacy

The Constitution of India did not explicitly guarantee 'Right to Privacy' as a fundamental right, but such a right was acknowledged by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*. Here, it was held that "*Right to Privacy is a fundamental right which is sewed under Article 21 of the Constitution*".[17] The Right to Privacy has become a monumental right considering that there have been some major social media and technological advancements in the recent past. Privacy has undoubtedly become an essential facet of life and without privacy, a *dignified life* cannot be guaranteed.[18] Privacy cuts across various fundamental rights and dignity is an essential element of all Fundamental Rights.[19] It has been five years since the *Puttaswamy* judgment upheld 'privacy' as a fundamental right, but the government is still debilitating in bringing forth a robust data protection law. This puts forward the question, "are we ready to barter the urgency for legislation with injury and harm?" It is now established that the current

[16]*Mardia Chemicals Ltd v Union of India* (2004) 4 SCC 311.
[17]*Justice K S Puttaswamy & Anr v Union of India & Ors* (2017) 10 SCC 1.
[18]Shiv Shankar Singh, 'Privacy and Data Protection in India: A Critical Assessment' (2011) 53 (4) Journal of the Indian Law Institute <http://www.jstor.org/stable/45148583> accessed 3 February 2023.
[19]*K S Puttaswamy v Union of India* (2017) 10 SCC 1.

Bill, if not amended, has great potential to obliterate the monumental right to privacy. Therefore, it becomes pertinent to see how and particularly which provisions do not ensure this very right. The Digital Personal Data Protection Bill, 2022 does not protect the fundamental right to privacy because of multiple reasons which include the following:

a. The Bill gives the Government the authority to make well-reasoned decisions exempting any government instrumentality from the Act's requirements in the "*interests of public order, state sovereignty, and national security*".[20]

b. There are exemptions granted in the interests of the security of the nation, if the exemptions adhere to the globally recognised standards of proportionality and necessity. Alternatively, under Clause 18 of the Bill,[21] any government institution may be able to conduct surveillance without any stated precautions with a simple Executive Order from the Central Government granting them access to the data.

This could result in grave invasion of citizens' privacy because it would shield the governmental institutions from the application of the statute. This is due to the fact that these standards are overly ambiguous and broad, making them susceptible to misunderstanding and abuse. Moreover, these broad exemptions did not adhere to the Guidelines established by the Supreme Court in the Puttaswamy case, where it held that standards curbing the 'Right to Privacy shall:

1) "*be substantiated by law,*
2) *serve a legitimate aim,*
3) *be proportionate to the objective of the law, and*
4) *have procedural protection against abuse*".[22]

[20]The Digital Personal Data Protection Bill 2021, cl 18(2)(a).
[21]ibid.
[22]*People's Union for Civil Liberties v Union of India* AIR 1997 SC 568.

According to Article 21, the basic 'right to life or personal liberty' is not unconditional protection, but is instead subject to legal procedures. The process must be just, reasonable, and equitable; it cannot be capricious, fantastical, or oppressive.[23] In other words, an individual's personal liberty may be taken away if the legal process used to carry out the action is just, equitable, and reasonable. Therefore, the right to privacy cannot be absolute. A law may infringe on the right to privacy, but it must pass the test for the restriction outlined in part III. The Bill, however, seems to be turning a deaf ear from these standards. Besides, stretching the horizon of exemptions in order to prevent any judicial or other scrutiny of the Government Instrumentalities' acts, which could lead to serious state violations of citizen privacy.

D. When arbitrariness met rule of law

The process of interpreting the rule of law in relation to the exercise of administrative authority has highlighted the importance of fair and just procedures, as well as proper safeguards against executive encroachment on human liberty.[24] The 'rule of law' is woven throughout the Indian Constitution and is one of its most fundamental elements.[25] The rule of law forbids arbitrariness, and its central tenet is *intelligence without passion* and *reason without desire*.[26] The rule of law is denied when there is arbitrariness or unreasonableness.[27] To put simply, tracing the arbitrariness across the various provisions of the Bill brings us to Clause 20(1)(b), which is a modified replica of the contentious Clause 86(1) of the prior Bill.[28] The provision empowers the government to delegate such functions to the Board as it may deem fit. However, the problematic part of the provision is that it neither

[23]*Maneka Gandhi v Union of India* AIR 1978 SC 597.
[24]*B Archana Reddy v State of AP* (2008) 6 SCC 1.
[25]*Merkur Island Shipping Corporation v Laughton* (1983) 2 AC 570 (CA).
[26]'Justice Bhagwati and Indian Administrative Law' (1959) 2(1) Journal of the Indian Law Institute <http://www.jstor.org/stable/43952781> accessed 12 December 2022.
[27]*BALCO Employees Union (Regd) v Union of India* (2002) 2 SCC 333.
[28]The Digital Personal Data Protection Bill 2021, cl 86(1).

prescribes the situations under which the government can exercise such a power, nor does it entail any limitations and safeguards to maintain the autonomy of the Board. The control (of any kind which impinges autonomy) of the Central government over the Board is out and out arbitrary and subsequently, antithetic to the rule of law.[29] In a nutshell, the moment an agency or authority acts arbitrarily and acts according to its whim and fancies without any reason and logic, such an act will become contrary to the basic tenet of Indian constitution i.e., rule of law.[30]

In *E.P. Royappa*, the court held that, "*Rule of law, Justice and fairness of equality conflicts with whim, fancies, unguided, illogical sense of arbitrariness"*.[31] In the context of the Bill, executive action under Clause 20(1)(b),[32] opposes the principle of rule of law. Because, when in a system regulated by rule of law, the free will is bestowed upon executive branch, it must be exercised within properly defined bounds, (totally absent in the present Bill) which means that judgments should be made using well-established principles and criteria.[33] The Constitution must be followed when using executive power.[34] If a decision is taken otherwise, it will become antithetic to a decision determined by the Rule of Law.[35]

III. A CAUTIOUS APPROACH: COMPARING GLOBAL EXAMPLES

Tracing back the access of data in times of Covid-19 and looking at the Bill through the lens of pandemic paints a gloomy picture. The pandemic has exposed the quest for robust data protection law to its

[29]*Nand Lal Bajaj v State of Punjab* (1981) 4 SCC 327.
[30]*Raman Dayal Shetty v International Airport Authority of India* AIR 1979 SC 1628.
[31]*EP Royappa v State of Tamil Nadu* 1974 4 SCC 3.
[32]The Digital Personal Data Protection Bill 2022, cl 20(1)(b).
[33]*SG Jaisinghani v Union of India and Ors* AIR 1967 SC 1427.
[34]*UNR Rao v Indira Gandhi* AIR 1971 SC 1002.
[35]*Shrimati Indira Nehru Gandhi v Shri Raj Narain* (1975) Supp SCC 1.

own challenges. Regimes all over the world have used coronavirus as an opportunity to demolish democratic structure. Even prior to the outbreak of Covid 19, we witnessed issues related but not limited to search engine manipulation and data leakages *viz*. Cambridge Analytica.[36] Therefore, it becomes pertinent to put the *status quo* of data protection law on the pedestal of monumental global trends and analyse its compatibility.

A. Takeaways from 'Cambridge Analytica' mayhem

A poor and ineffective data protection legislation will cause more harm than none at all because it will legalize invasions of privacy and monitoring, and would prevent citizens from accessing legal recourse. Having witnessed the Cambridge Analytica havoc, which has provided a prologue to the effect of search engine manipulation,[37] and its role in affecting the 2016 US elections, wherein there was unauthorized access to the data of thousands of Facebook users which stirred political conundrums, it would not be right to put this conjecture to rest entirely.[38] The Cambridge Analytica scandal highlighted how personal data can be harvested without consent and used for targeted political messaging. In a like matter, in a democratic country like India, where privacy rights are not well protected, citizens' personal information could be exploited for political gain or manipulation. Besides, the exemption granted to government agencies to access citizen data could not only lead to increased government surveillance but there is a higher

[36]K. Harbath, 'History of the Cambridge Analytica Controversy' (*Bipartisan Policy Center*, 16 March 2023) <https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/> accessed July 2023.

[37]Rogers K and Bromwich JE, 'The Hoaxes, Fake News and Misinformation We Saw on Election Day' (*The New York Times*, 8 November 2016) <https://www.nytimes.com/2016/11/09/us/politics/debunk-fake-news-election-day.html> accessed 16 December 2022.

[38]'Facebook to Contact 87 Million Users Affected by Data Breach' (*The Guardian*, 8 April 2018) <https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach> accessed 16 December 2022.

risk that political actors could use such collected data to tailor messages to specific voter segments, potentially distorting the electoral landscape.

Therefore, the exemptions to the government instrumentalities is an opportunity to ensure that such manipulation is concealed and that no traces of manipulation are left behind.[39] The potential use of technology in elections by having access to personal data of the voters is a direct threat to the democratic structure of the country.[40] Therefore, by not connecting these dots, a distorted picture of democracy would be painted where the "*choice of the people, by the people and of the people*" are all guided by the data-driven puppeteers. Thus, it becomes apposite to bear this in our minds that a law that enables government agencies from accessing sensitive personal information about its residents will have a negative impact on political power struggles and destroy India's democratic setting.

B. Pandemic meets privacy

As the Covid-19 pandemic surfaced, regimes around the world came up with different approaches to contain the contagion. The democratic states resorted to a not-so-democratic approach to curb the virus.[41] Some scholars even remarked that the pandemic lifted the authoritarian veil of various democratic governments.[42] Governments around the

[39]The Digital Personal Data Protection Bill 2022, cl 18(2)(a).

[40]Snow J, 'Last Year, Social Media Was Used to Influence Elections in at Least 18 Countries' (*MIT Technology Review*, 30 June 2022) <https://www.technologyreview.com/2017/11/14/3847/last-year-social-media-was-used-to-influence-elections-in-at-least-18-countries/> accessed 12 December 2022.

[41]Chinglen Laishram and Pawan Kumar, 'Democracies or Authoritarians? Regime Differences in the Efficacy of Handling Covid-19 in 158 Countries' (2021) 67(3) Indian Journal of Public Administration <https://doi.org/10.1177/00195561211042977> accessed 20 December 2022.

[42]Amy Slipowitz, 'The Devastating Impact of Covid-19 on Democracy: Think Global Health' (*Council on Foreign Relations*, 27 September 2021) <https://www.thinkglobalhealth.org/article/devastating-impact-covid-19-democracy> accessed 19 December 2022.

world used contact tracing applications to collect data in order to monitor the spread of the virus.[43] The Indian government also used a mobile app called *Aarogya Setu*[44] to keep track of people who have come into touch with sick people. All these applications were released with the goal of containing the COVID-19 infection as well as to show potential hotspots. These mobile applications keep track of the information of anyone who has interacted with another person during the course of their daily activities so that, in the event that one of them tests positive for COVID-19 in the future, the other person can be informed and take prompt action to seek medical attention. Demographic information, contact information, self-evaluation information, and location information were all included in the details of the people and are referred to as *Response Data*. Although contact tracing is a crucial step in halting the virus's transmission, privacy issues regarding the people whose data has been watched have been brought up. In the absence of any data protection law, there was no safeguard against such data leakage during health emergencies like Covid-19 in India. It is to be noted that the prior Bill was under review by the Joint Parliamentary Committee during the first and second waves of Covid-19.

Even so, the current Bill contains no safeguard against protection of data during health emergencies. *Per contra*, the Bill vide Clause 8(5)[45] provides that the consent of the data principal is deemed for "*taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat*

[43]Osama Shaikh and Huzaifa Shaikh, 'Covid-19 and Challenges to Economic Models and Political Regımes' (2021) 4(1) ARHUSS.

[44]Bhaskar Pant and Amit Lal, 'Aarogya Setu App: A Tale of the Complex Challenges of a Rights-Based Regime' (*The Wire,* 11 May 2020) <https://thewire.in/tech/aarogya-setu-app-challenges-rights-based-regime#:~:text=tech-,Aarogya%20Setu%20App%3A%20A%20Tale%20of%20the%20Complex%20Challenges%20of,structures%20at%20a%20larger%20scale.> accessed 20 December 2022.

[45]The Digital Personal Data Protection Bill 2022, cl 8(5).

to public health" which unequivocally allows non-consensual processing of data during health emergencies. Besides, the gathering of sensitive information such as contact, location, and health data, poses serious hazards to citizens. People whose personal information is being gathered can be worried about who will get access to and use their data, how that data might be used, how that data might be shared with other entities, and what security precautions will be taken to protect that data from loss or misuse. Therefore, the lack of specific and informed consent from the data principal could lead to excessive processing of the personal data that was gathered.[46] Furthermore, because the processing would occur without consent, the data principal is not at liberty to revoke the consent at any time.[47] In a nutshell, data monitoring has proved to be a useful tool, but it is also imperative that consent is the foundational framework of data protection law and any deviation from it needs to be tailored narrowly.

IV. TESTING THE COMPATIBILITY OF THE CURRENT BILL WITH EU GDPR

The European Union GDPR,[48] and the DPDP Bill are two most important data protection Regulations in the world. The common denominator of both the Regulations is to protect the personal data of individuals and provide them with control over how their data is used and processed. The data protection Regulation in India has always looked up to EU GDPR and the provisions of the earlier Bill were also inspired by the EU regulation.[49] There are shreds of EU GDPR in the

[46]Vinay Narayan, 'DPDP Bill 2022: 'Deemed' Consent, To Users' (*MediaNama*, 12 December 2022) <https://www.medianama.com/2022/12/223-dpdp-bill-2022-deemed-consent-to-users-detriment-views/> accessed 2 January 2023.
[47]ibid.
[48]Regulation (EU) 2016/679.
[49]'Comparison: Indian Personal Data Protection Bill 2019 vs GDPR' <https://www.privacysecurityacademy.com/wp-content/uploads/2020/05/Comparison-Chart-GDPR-vs.-India-PDPB-2019-Jan.-16-2020.pdf> accessed 4 January 2023.

current Bill as well, therefore, it is apposite to consider how compatible the present Bill is with respect to EU GDPR.

Firstly, on a larger scale, the main distinction is that, regardless of where the entity is located, the GDPR pertains to all entities operating in the EU and processing personal data of EU citizens.[50] The DPDP Bill, on the other hand, only applies to data controllers and processors located in India.[51] Secondly, the DPDP Bill describes personal data as information about or relating to a *natural person* that can enable that person to be identified; however, under the GDPR, any information "*relating to an identified or identifiable natural person*" is regarded as personal data. Besides, the GDPR requires that individuals must give their explicit and informed consent for their data to be processed. The DPDP Bill, on the other hand, requires data controllers to obtain consent from individuals, but the level of detail required for such consent is not specified, which is again an entirely different moot point.

A. Comparing the common denominators of EU GDPR with DPDP Bill

a. **Data Breaches:** In GDPR, data controllers must notify the appropriate authorities of a personal data violation within 72 hours of becoming aware of it.[52] Similarly, the DPDP Bill not only requires data controllers to report breaches to the relevant authorities, but also requires them to inform the affected individuals without undue delay, which is one of the positives of the Bill.[53]

[50]'EU General Data Protection Regulation (GDPR)' (*EU General Data Protection Regulation (GDPR) - Definition - Trend Micro IN*) <https://www.trendmicro.com/vinfo/in/security/definition/eu-general-data-protection-regulation-gdpr#:~:text=The%20GDPR%20will%20also%20apply,personal%20data%20of%20EU%20citizens> accessed 2 January 2023.
[51]The Digital Personal Data Protection Bill 2022, cl 4(1).
[52]GDPR, Regulation (EU) 2016, art 33(1).
[53]The Digital Personal Data Protection Bill 2022, cl 9(5).

b. **Data Portability:** The GDPR gives the right to transmit personal information in machine-readable format.[54] The DPDP Bill does not specifically mention the right to portability of the data.

c. **Right to be Forgotten:** Under certain circumstances, individuals have the authority to have their personal data destroyed under the GDPR.[55] The DPDP Bill grants the right to limit or stop the processing of an individual's data under the proposed law, but does not specifically mention the right to be forgotten.[56]

d. **Penalties:** Amount of 20 million euros or up to 4% of a company's global yearly turnover, whichever is higher, may be fined for non-compliance under the GDPR.[57] Lower penalties for non-compliance are provided by the DPDP Bill.[58]

In a nutshell, both the GDPR and the DPDP Bill aim to protect personal data and give individuals control over how their data is used and processed. However, the GDPR has a broader scope and provides for higher penalties for non-compliance, while the DPDP Bill is more specific to India and has lower penalties, which questions the comprehensiveness in light of existing and upcoming challenges.

V. CONCLUSION & RECOMMENDATIONS

The non-presence of a comprehensive data protection law in India pictures an *Orwellian state* and is out and out in violation of the fundamental right to privacy. The existing legal vacuum makes the entire country susceptible to several threats. Due to the absence of robust data protection regulation, there are various challenges

[54]Luke Irwin, 'The GDPR: Understanding the Right to Data Portability' (*IT Governance Blog*, 9 June 2020) <*https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-right-to-data-portability*> accessed 5 January 2023.
[55]GDPR, Regulation (EU) 2016, art 17(1).
[56]The Digital Personal Data Protection Bill 2022, cl 7(5).
[57]GDPR, Regulation (EU) 2016, art 83(6).
[58]The Digital Personal Data Protection Bill 2022, cl 25(1).

especially with regards to data collection, regulation, storage, and use by private companies and government agencies, among other things.

Therefore, it becomes abundantly clear that we are in dire need of a strong legislation to deal with the current and upcoming challenges. Now, as far as the current status of the Regulation is concerned, we have seen how the Bill vide Clause 8(2) grants exclusive rights to the state to process the data in a non-consensual manner. We have also seen how the exemption to the government agencies vide Clause 18(2)(a) and the Central Government's control over the autonomy of the Data Protection Board as provided under Clause 20(1)(b) debilitates the independent structure of the board and besides, we have also seen how the current law does not fulfil the very objective for what it is being enacted. *Per contra*, we could also see some positives in the draft. The Bill contains the provision which requires the data fiduciaries to mandatorily notify the data principal in the event of compromise with their data. This has addressed one of the major issues in the earlier drafts. Another positive of the Bill is that now, strong barricading has been imposed upon the processing of children's data.

Despite these positives, the negatives of the Bill weigh heavier, which substantiates the argument of the authors with regard to how an ineffective data protection Regulation will be deadlier than no Regulation at all. Bringing forth the Regulation in its current form will not only fail to achieve its primary object, but will also legalise the arbitrariness, thereby invading one of the most quintessential and monumental rights, i.e. Right to privacy. In conclusion, the authors assert that the current status of the Bill needs a total revamp, as even after undergoing an overhaul, the Regulation still has some major flaws. It is concluded that the current Bill is the adulterated adaptation of the earlier Bills which makes it more shallow on multiple factors which includes notice requirements, exemptions to government instrumentalities with no safeguards, pretentious independence of the Data Protection Board, right to be forgotten among other things.

The following suggestions flow from the numerous shortcomings of the DPDP Bill which includes:

Firstly, the inclusion of the term 'as may be prescribed' in the legislation which regulate individual's data could lead to varying interpretations of data protection standards thereby, potentially impacting transparency and accountability. Therefore, the primary recommendation is that the term 'as may be prescribed' must be worded clearly so that several crucial provisions are not left to executive rulemaking without legislative guidance at a later stage.

Secondly, according to Clause 8, if it is considered necessary, a data principal is said to have consented to the processing of her personal data. The provision contains the circumstances under which consent is deemed to have been provided, but there are no procedural safeguards against the same. Therefore, it is strongly recommended that there should be the application of Clause 7 (4) which prescribes 'withdrawal of consent' in the provision of 'deemed consent' as well.

Lastly, the current Bill gives exemptions to State and private data fiduciaries for processing of the data, which has been one of the most contentious points of the earlier as well as current draft. Therefore, it is strongly recommended that the exemptions must be given to the State as well as private data fiduciaries only when they fulfil the factors of proportionality and necessity.