DATA PROTECTION IN INDIA: A SERIES OF FLAWED ATTEMPTS

Ritisha Sinha & Vidushi
2nd year BA LLB students, National Law University, Delhi.
ritisha.sinha21@nludelhi.ac.in & vidushi.21@nludelhi.ac.in

Abstract

The domain of data privacy in India has lagged behind not just the other countries, but also the technological developments in the present times. This, however, does not insinuate the lack of efforts to come up with a comprehensive data protection regime, rather it reflects the inability to come up with one that appropriately suits the interests of the citizens. Taking into perspective all the measures taken so far, this paper aims to analyse the newly released Draft Digital Personal Data Protection Bill, 2022. In delineating this analysis, the draft bill's conformity with the Constitution of India is judged and the ambiguity in the terminologies used therein that can grant excessive power to the Union Government is critically examined. The paper, in all, makes an effort to trace the history of the Data protection regime and delve into the Draft DPDP Bill, 2022, which has been presented forward as a progressive and laudable move for the protection of Privacy.

Keywords: Privacy, Legislation, Fundamental Rights, Personal Data.

1. Introduction

As they say, Data is the new oil. With the advent of technology and the Internet, Indian privacy jurisprudence developed, and the protection of data turned out to be of paramount importance. The age of Information has resulted in complex issues for informational privacy, which arises due to the nature of Information itself. Still, it took us subsequent Supreme Court Judgements, numerous attempts by the Legislature and over 70 years of Independence to explicitly declare Privacy as a Fundamental Right, which lies at the foundation of every Data Protection Law.

After the insufficiency of these attempts, the Digital Personal Data Protection Bill has been released to lay down a data protection regime in India. While the bill is being observed and tracked by the interested stakeholders in India as a whole, it is imperative to understand the history of the efforts that have led us here. From *Govind vs State of Madhya Pradesh(1975)* to the landmark case of *K.S Puttaswamy vs Union of India(2017),* the Hon'ble Supreme Court has always reiterated that the Right to Privacy forms an inalienable part of Article 21 of the Indian Constitution.

The ever-expanding Right to Life and Personal Liberty recognises the Right to Privacy, which extends its protection to all forms of data that a person identifies oneself with. Other than the constant measures by the judiciary, there have been not-so-sincere attempts by the legislature too. From the introduction of the IT Act 2000, which focused on financial protection, there was hardly any comprehensive and exhaustive legislation that could safeguard the privacy of an individual, especially against excesses of the government. With data protection only as an ancillary function, the act could have hardly fulfilled the necessary functions of a law that had the function as its core. To remedy the situation, an amendment to the act was brought in 2008, which yet again primarily addressed corporate bodies, later followed by Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or information) Rules, 2011. The need for comprehensive legislation was soon realised, and the Personal Data Protection Bill 2019 was presented in Parliament. With some shortcomings coming to the light, the bill underwent reforms; however, it was, in the end, withdrawn. All of such attempts in their entirety have not been enough to ensure the protection of data. The spirit of the legislature had nevertheless not dampened and the same was manifested in the form of another bill.

In its quest for a Data Protection Law, the Government of India released the Draft Digital Personal Data Protection Bill in November 2022 (after withdrawing the Personal Data Protection Bill, 2019) to seek suggestions on the same. Fourth in the sequence of such data protection bills that the Government of India has released over the years, the bill is more cryptic than it appears to be. The introduction of any Data Protection Bill must certainly aim at strengthening the rights of the citizens and endorsing the pertinent principles of Data Protection, as declared in the *Puttaswamy* case. Among the most contentious elements of the bill are Sections 8, 18, 19, and 30, which envisage introducing the concept of 'Deemed Consent', providing wide exemptions to Government agencies, creating the Data Protection Board and amending the Right to Information Act, respectively.

Contrary to the Constitutional provisions under Articles 14, 19 and 21, certain sections of the bill promote State Surveillance and Disproportionate use of Executive powers.

To say the least, the bill may be necessary to fill the void created by the withdrawal of the PDP Bill, 2019 but is certainly insufficient for the assertion and enjoyment of the Right to Privacy in its entirety.

This essay presents an analytical and chronological history of the Indian Supreme Court's engagement with the Right to Privacy and the unfolding of Data Protection Jurisprudence. The paper does not limit itself to the bill and also presents a probe into the past efforts made and what led to their failure.

This is also accompanied by an in-depth comparison with a major data protection framework - GDPR. Through various chapters, this paper aims to analyse the repercussions in case this Draft Bill (without any substantial improvements) eventually passes to become an Act. The present draft does its best to compromise the undeniable principles of Data Protection, such as Purpose Limitation and Data Minimisation and therefore denies the citizens their rights. By throwing light on some of the provisions, the paper tries to study their potential implications on Fundamental rights and how they can conceivably affect the much-revered Constitutional principles of Proportionality, Division of Power, Due Process and Non-Arbitrariness. Such a comprehensive understanding of the evolution of Data Protection Laws in India is cardinal to making a case for the better protection of human life and dignity and enjoyment of fundamental rights to its fullest.

2. Tracing the History of Data Protection.

The DPDP, better known as the Digital Personal Data Protection Bill, was released by MEITY in 2022.[1] The bill is another effort by the government to come up with data protection legislation around four years after the last Personal Data Protection Bill, 2019 (PDP bill) that was withdrawn by the government. Considering the concept of the right to privacy, it is imperative to pay heed to the introduction of legislation related to the protection of privacy and critically analyse it. However, before proceeding with the analysis, comprehending the background and historical information related to the bill must be brought into the limelight to observe whether it is consistent with the developments taking place or falls short of the promises made.

The Indian data protection framework is unable to keep up with the world's rapid change, with technology becoming an all-pervasive phenomenon. It is obvious that the current legal system is inadequate to handle this significant task.[2] If paying close attention, it can be noticed that India has had four main developments for handling data protection. Along with it, there have been some subsidiary efforts too. The major developments so far have been:

1) Introduction of IT Act, 2000 and 2008 amendment
2) SPDI rules, 2011
3) *KS Puttaswamy's* judgement

[1] Nishtha Badgamia, Explained: What Is India's Digital Data Protection Bill, 2022 All About?, WION, December 21, 2022, https://www.wionews.com/india-news/explained-experts-raise-concerns-about-indias-digital-data-protection-bill-2022-545276 (Last visited on March 27, 2023)

[2] Ashit Kumar Srivastava, *Data Protection Law in India: The Search for Goldilocks Effect*, 5 Eur. Data Prot. L. Rev. 408 (2019)

4) PDP bill, 2019 – withdrawn

It is important to discuss each one in detail to understand their limited nature and how they did not suffice either individually or together for constituting an exhaustive data protection regime.

2.1 IT ACT: The IT Act's primary goal was to promote electronic trade in India, not to shield a person from the dangers of manipulating data or targeted advertising. Given the limited reach of the IT Act, protection against using and transmitting data for manipulating elections and automated control looks like an unrealistic goal. It primarily focused on the fundamental financial protection in the online transaction sector, which is one component of data protection. The "state" is barely ever mentioned in the IT Act, which primarily deals with corporate bodies. Given the actual truth, it is difficult to accept that there should only be data protection legislation that applies to citizens and non-state actors, as the notion that the state would always serve as a welfare institution and protector is undoubtedly busted. Later, sections 43A[3] and 72A[4] of the IT Act 2000 were added by the passage of the IT Amendment Act, 2008. The primary goal of these new regulations was to safeguard the person against the dangers associated with managing, processing, and storing sensitive personal data. Interestingly, this clause of the modified IT Act 2008, as described in view of the IT Act 2000, yet again primarily addressed corporate bodies.

2.2 SPDI RULES: The 2008 amendment's failure to specify "sensitive personal data or information" was one of its biggest flaws, which lessened the section's overall beneficial impact. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, were created by the Ministry of Communications and Information Technology to fill this gap and resolve the pressing need for definition clarification. These regulations, which offered a thorough description of sensitive personal data, were created in the course of carrying out the authority granted by section 43 A of the IT Act.[5] The definition given, however, was quite narrow in comparison to comparable legislations like GDPR. Also, another drawback of these rules was in its definition of “reasonable security practice and procedure”. According to it, if a complete agreement is present between the customer and the corporation that provides services, the stipulations of the SPDI rules

[3] Information Technology (Amendments) Act, 2008, § 43A, No. 10, Acts of Parliament, 2009 (India).
[4] Information Technology (Amendments) Act, 2008, § 72A, No. 10, Acts of Parliament, 2009 (India).
[5] Asang Wankhede, *Data Protection in India and the EU: Insights in Recent Trends and Issues in the Protection of Personal Data*, 2 Eur. Data Prot. L. Rev. 70 (2016)

can be readily avoided. The user's only option is frequently to click the "I Agree" option to accept the company's policies because it is extremely clear that the customer's negotiating power is comparatively low compared to the companies providing the services[6]. These rules could not alone provide a comprehensive data protection framework either.

2.3 ***K.S. PUTTASWAMY V. UNION OF INDIA*** [7]: Retired Justice K.S. Puttaswamy's petition to the Honourable Supreme Court is where the latest litigation history of India's data security policy may be properly tracked. It was held that the right to privacy is safeguarded under Article 21 of the Constitution [8] under the right to life and personal liberty. The right to privacy was deemed to be a fundamental right in this judgement, albeit with reasonable constraints, such as legality, need, and proportionality. The Supreme Court even ruled that the government must create a data protection law in order to deal with issues with privacy in modern digitalised times.[9]

2.4 PDP BILL, 2019: After the above judgement, the B N Krishna Committee presented the PDP bill's initial draft in a report that was published in 2018. After undergoing numerous changes and consultations, the Krishna Committee's suggestions and the draft PDP were both tabled in Parliament in 2019.[10] The proposed Personal Data Protection Bill 2019 was on the lines of GDPR, which is now widely recognised as a model for privacy and data protection laws around the globe. Despite this, some conspicuous shortcomings got the bill criticised. The bill granted access to non-personal data to the government. It was contended that the government should not have been given the authority to request any non-personal data from businesses and that non-personal data should have been dealt with in a separate bill. This bill gave the government access to commercial information that may not be personal information. Still, such information might have been crucial from a business standpoint, such as information on intellectual property, corporate strategy, and mergers and acquisitions. The global investor community certainly received a bad message from the exception granted to government agencies; this needed to be addressed.[11] Users, corporations, and the government are the key stakeholders involved in these deliberations. They must all get around the table and come to an

[6] Srivastava, *supra* note 3.
[7] *Justice K.S.Puttaswamy(Retd) vs Union Of India, AIR 2017 SC 4161.*
[8] INDIA CONST. art 21.
[9] Sameer Kumar Dwivedi, *From Privacy to Data Protection in India: Evaluating the Personal Data Protection Bill, 2019*, 3 Int'l J.L. Mgmt. & Human. 2136 (2020)
[10] Ayushi Kar, The Withdrawal Of The PDP Bill And The Road Ahead, THE HINDU BUSINESSLINE, August 8 2022, https://www.thehindubusinessline.com/blexplainer/the-withdrawal-of-the-pdp-bill-and-the-road-ahead/article65747464.ece (Last visited on March 27, 2023)
[11] Sameer, *supra* note 9.

agreement. With the PDP Bill 2019, it appeared the situation was different. Careful examination of sections 13, 14, 19, and 20 showed that these were facilitating measures in the government's interest, giving it the ability to obtain the private data of its residents in the guise of the public good.[12] Standards of necessity were also absent from this bill, and it laid out requirements for "exemption of certain laws for specific processing of personal data" that established the conditions under which government agencies must be granted access to citizens' personal data. In this case, the proportionality principle mandated that the officials find an equilibrium between the tools at their disposal and the goals they have in mind. The goal of this law was "to protect the individual's right," but due to this provision, the new legislation offered an opportunity to intrude on the individual's privacy. This exemption raised questions about state surveillance of personal data and sparked a new discussion about the government's meddling.

After the PDP bill was withdrawn, the DPDP bill was proposed three months later.[13] The new bill aimed to reform the questions raised over the PDP bill. The particulars of the new bill will be discussed in later chapters.

3. Comparison With GDPR And Its Analysis.

GDPR is a regulation in accordance with which companies must safeguard the privacy and personal information of EU people when conducting business in the EU.[14] The GDPR, which replaced an out-of-date data privacy directive from 1995, was adopted in 2016.[15] For exchanges within EU countries, it contains regulations that demand firms preserve the personal information and privacy of EU individuals. The new DPDP bill and the previous PDP bill also drew out measures from this law and adopted them for framing the data protection law in India. But their effectiveness and comparison need to be gauged to analyse the present bill in the discussion properly. While keeping this in mind, the observation regarding these laws will be made. All in all, the chapter addresses the following points: Is the GDPR a perfect standard for India? Is India drawing out provisions from GDPR well, and what is the comparison between the two?

[12] Ashit Kumar Srivastava, *Data Protection Law In India: The Search For Goldilocks Effect*, 5 Eur. Data Prot. L. Rev. 408 (2019)
[13] Drishti IAS, *Digital Data Protection Bill, 2022*, November 21, 2022, https://www.drishtiias.com/daily-updates/daily-news-analysis/digital-personal-data-protection-bill-2022 (Last visited on March 20, 2023).
[14] Michael Nadeau, What Is The GDPR, Its Requirements And Facts?, CSO ONLINE, June 12 2020, https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html (Last visited on March 20, 2023)
[15] Id.

Firstly, efforts should be made to understand the legal framework to be able to figure out the shortfalls. The GDPR governs the transfer of personal data beyond the EU as well.[16] It aims to enforce a single data security law across all Eurozone countries, eliminating the requirement for individual member states to create their own data protection regulations and ensuring that all EU regulations are identical. It is significant to remember that, in conjunction with EU members, any business, irrespective of location, that promotes goods or services to EU people is governed by the rule. As a consequence of this, GDPR will affect data protection obligations across the board.

3.1 Is GDPR a Sufficient and Reliable Standard?

GDPR has been widely accepted as a standard for data protection laws by many countries. Despite this, the law suffers from some deficiencies that have affected its implementation. Such gaps can be attributed to vagueness in the interpretation of the language of the law and further delays in execution. The insufficiency of GDPR can be impute to:

The GDPR offers a lot of room for interpretation: One of the largest barriers to conformity is the GDPR's ongoing ambiguity in some places. A significant portion of GDPR is open to interpretation. It states that businesses must offer a "reasonable" level of security for personal data. Still, it doesn't specify what "reasonable" means.[17] Unspecified phrases like "disproportionate effort," "likelihood of (high) risk to rights and freedoms," and "undue delay" may still need more clarification by the judiciary or authorities, or years for specific market practices to emerge.[18] This allows the organisation in charge of enforcing GDPR much discretion when deciding how much to fine companies for privacy violations and other violations.

Existing uncertainty: The previous problem feeds the problem of ambiguity along with other factors. This would take a while for distinguishable examples to be created because regulators have acknowledged that they lack the means to deal with the number of reported violations they get.[19] The apparent disparity in how sanctions are applied across the various ICOs only serves to increase that ambiguity. "Ask two different regulators how GDPR fines should be calculated, and you will get two different answers. We are years away from having legal certainty on this crucial question," Patrick

[16] GDPR.EU , *What Is GDPR, The Eu's New Data Protection Law?*, https://gdpr.eu/what-is-gdpr/ (March 20, 2023).
[17] Nadeau, *supra note 14.*
[18] Thomson Reuters, *Top Five concerns with GDPR compliance*, https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance (Last visited on March 20, 2023).
[19] Id.

Van Eecke, the head of DLA Piper's global data protection practice, made this statement in the business report.

Inaction and delay: The action thus far is insufficient and late for activists still expecting authorities to decide on a plethora of complaints they lodged more than two years ago. [20] In a previous statement, Austrian data security campaigner Max Schrems said that after an initial moment of confusion, a substantial section of the data sector has learned to cope with GDPR despite not truly changing practices. [21] He said that out of the roughly 50 cross-border lawsuits his activist group has brought in the previous four years, none had yet received a verdict.

3.2 Comparison

- It is important to note that Chapter 5 of the GDPR lays out a thorough process for cross-border data movement. Adequacy judgements, established regulations, common contracts, and derogation provisions are used to carry this out. On the contrary, the DPDP Bill only briefly and indefinitely addressed the concept of cross-border data transmission. Additionally, the notion of data localisation, which was prevalent in the earlier draughts, is not mentioned. Personal data may now be transferred "freely" to "trusted" jurisdictions that will be informed later.[22]
- It should be highlighted that the DPDPB's dependence on the mechanism for notice and permission, which is comparable to the EU GDPR, is troublesome. Users are frequently ignorant of the true purposes for which their data is used, even when they are given a warning. Additionally, the constant barrage of consent notices makes users assent to everything automatically, which results in consent fatigue. The DPDPB has acknowledged "consent managers," or data fiduciaries, who will assist users in managing their consent in an effort to address this problem. One expects that this will be the first step in India toward a greater comprehensive legal recognition of data custodians/mediators that interact and bargain with stakeholders on behalf of data principals.[23]

[20] Vincent Manancourt, What's Wrong With The Gdpr?, POLITICO, June 15, 2022, https://www.politico.eu/article/wojciech-wiewiorowski-gdpr-brussels-eu-data-protection-regulation-privacy/(LastMarch 20, 2023)

[21] Id.

[22] Raj Shekhar & Aman Yuvraj Choudhary, Digital Personal Data Protection Bill Vis-À-Vis GDPR, INDIACORPLAW, November 29, 2022, https://indiacorplaw.in/2022/11/digital-personal-data-protection-bill-vis-a-vis-gdpr.html (Last visited on Mach. 20, 2023).

[23] Vinay Narayan, 'Deemed Consent' Provision In Data Protection Bill Is To Users' Detriment, MEDIANAMA, December 12, 2022,

- The GDPR has chosen a different level approach for the consent necessary for handling children's personal data. Based on the Member State, the minimum age for legal consent in such circumstances varies from 13 to 16 years. Furthermore, it is the obligation of the organisation to obtain parental consent to make a reasonable attempt to confirm that the parent truly gave consent. The DPDP Bill, like the previous efforts at making similar legislations, relies on the absolute age of 18 to provide valid permission and fails to examine the tiered approach that is used widely around the world.[24]
- The GDPR is in charge of data protection in the EU and requires each member state to establish a separate supervisory authority to oversee how the legislation is being implemented. The regulations clearly outline the functions and responsibilities of the supervising authority as well as the process for choosing its members. But in India, the national government has enormous authority over everything from creating the Data Protection Board to determining the board's mandate and responsibilities. As a result, the government has more influence over the envisaged DPB because it will choose its members, establish the terms of their employment, and specify the duties they will carry out.[25]

The analysis of the shortfalls of the GDPR puts forward the issues that the DPDP bill might have adopted too in matters of implementation. As good as a standard GDPR might have laid down, it has its own flaws. The problem of ambiguity is that this is not exclusive to GDPR and raises concerns for the Digital Personal Data Protection Bill, 2022, too. This, again, is not the only issue. The present bill, when compared to GDPR, shows that the bill has not been able to keep up with it in various aspects. The inability to be able to adopt the exemplary portions of the GDPR, while the possibility of not being able to remove the gaps remains, is a major problem that the bill might suffer from. With the GDPR bill being more sensitive to ascribing limited power to the government of the land, the absence of the same in the DPDP Bill is glaring. Other concerns, as mapped out above, are similarly alarming. The result, as such, presents the areas that can be reformed and

https://www.medianama.com/2022/12/223-dpdp-bill-2022-deemed-consent-to-users-detriment-views/ (Last visited on March 20, 2023)

[24] Raj, *supra* note 22.

[25] Dalima Pushkarna, Digital Personal Data Protection Bill: Way To An Ambiguous Data Protection Regime In India?, JURIST, December 23, 2022, https://www.jurist.org/commentary/2022/12/dalima-pushkarna-digital-personal-data-protection-bill/ (Last visited on March 20, 2023).

worked upon so that the bill better suits the needs of the people and holds up to protecting the data.

4. Does the Draft Digital Personal Data Protection Bill, 2022 Conform With Part III Of The Indian Constitution?

The recent release of the Draft Digital Data Protection Bill, 2022 has raised certain questions about the future of Data Protection in India and whether the bill does anything to respect citizens' fundamental rights or not. Because Information is Non-rivalrous, Invisible and Recombinant, it dodges any attempt made at channelizing and administering it. Information is non-rivalrous in the sense that there can be simultaneous users of the good- the use of a piece of information by one person does not make it less available to another and invisible in the sense that invasions of data privacy are difficult to detect, and it can be accessed, stored and disseminated without notice. Moreover, information is recombinant as the data output can be used as an input to generate more data output.[26]

In order to determine if the provisions of the Digital Personal Data Protection Bill pass constitutional scrutiny, this chapter will examine them against Puttaswamy, other similar legal rulings and some pertinent constitutional provisions. Despite the bill's praiseworthy efforts to achieve compliance with international data protection standards, it has a number of flaws that call into doubt its legitimacy.[27] Numerous provisions of the bill suffer from manifest arbitrariness, and unreasonableness, violate Articles 14 and 21 of the Constitution and give disproportionate powers to the executive over the legislature.

4.1 Violation of Article 14

A look at Section 8 of the draft bill brings to us the concept of 'Deemed Consent'. Euphemistically called 'Deemed consent', this provision provides a wide range of circumstances where an individual's data may be collected, stored and processed without their express consent.[28] Section 8 of the Data Protection Bill, 2022 presupposes the data principal's consent if "such processing is necessary" and then goes on to list a plethora of extremely broad circumstances in which processing may be justified, including "where it is reasonably expected" (section 8(1)) that personal data would be

[26] Christina P. Moniodis, *Moving from Nixon to NASA: Privacy's Second Strand – A Right to informational privacy*, 15 YJoLT 1. 153 (2012).

[27] Siddhant Verma, The Data protection bill is riddled with arbitrary provisions that violate the right to privacy, THE WIRE, January 2, 2023, https://thewire.in/rights/data-protection-bill-arbitrary-provisions-right-to-privacy. (Last visited on March 20, 2023).

[28] Gautam Bhatia, Why the New Draft Data bill must be reconsidered, HINDUSTAN TIMES, November 29, 2022, https://www.hindustantimes.com/opinion/why-the-new-draft-data-bill-must-be-reconsidered-101669731526700.html (Last visited on March 20, 2023)

provided, "for the provision of any service or benefit to the Data Principal," (section 8(2)) or even just "for employment," (section 8(7)) as well as when it is in the public interest (section 8(8)[29]. Even more grossly surprising is Section 8(9), which allows for the assumption of consent "for any fair and reasonable purpose *as may be prescribed*", with very inadequate safeguards. The explanatory note that came along with the Bill says that the concept of deemed consent has been introduced for "*seeking the consent of Data Principal when it is impracticable or inadvisable due to pressing concerns*" in many situations. The note further mentions that "*clearly defined situations wherein insisting on consent would be counterproductive have been listed under the Bill*".[30] These broad terms do not have a definite meaning and also cannot be restricted to one interpretation. The lack of clarity in these terminologies also provides leeway to the state to operate in opacity, exacerbated in the absence of an oversight mechanism, which doesn't go beyond the same department.[31]

The conditions and situations cited for the purpose of 'Deemed Consent' are arbitrary and violate Article 14 of the Constitution which strictly warns against the arbitrary and discriminate use of powers. Under Sec. 18(2) of the Act, the central govt can exempt any instrumentality of the state from compliance with the law "in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these."[32] This would give the notified govt. instrumentalities immunity from the application of the law, which could result in immense violations of citizen privacy.[33] These situations seem to be vaguely defined and the provision appears to be extremely wide in scope which makes it susceptible to misuse and can potentially authorise vast and unchecked data mining, without constraint.

Moreover, under sec. 19, the Act provides for a Data Protection Board of India whose "strength, the composition of the Board and the process of

[29] Singh, M. and Kaur, S., The Digital Personal Data Protection bill 2022 - A Snapshot, Lexology, LEXORBIS, December 26, 2022, https://www.lexology.com/library/detail.aspx?g=2f61e212-201a-4d95-8253-8fc8f3f010b9 (Mar. 20, 2023).

[30] Draft Digital Personal Data Protection Bill, 2022, § 8(9) (India).

[31] Kamesh Shekhar, Shefali Mehta, The state of surveillance in India: National security at the cost of privacy ORF, February 17, 2022, https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india/ (Last visited on March 20, 2023)

[32] Draft Digital Personal Data Protection Bill, 2022, § 18(2) (India).

[33] Tanmay Singh, The DPDPB, 2022 does not satisfy the Supreme Court's Puttaswamy principles, INTERNET FREEDOM FOUNDATION, December 16, 2022, https://internetfreedom.in/the-digital-personal-data-protection-bill-2022-does-not-satisfy-the-supreme-courts-puttaswamy-principles/ (Last visited on March 20, 2023)

selection, terms and conditions of appointment and service, removal of its Chairperson and other Members shall be such as may be prescribed"[34]. An excess delegation of power to the central govt. without proper guidelines by the legislature is in itself arbitrary.[35] The virtue of non-arbitrariness in Art. 14 was recognised in *S.G. Jaisinghani v. Union of India*[36] where the Court held that "absence of arbitrary power" as sine qua non to the Rule of law with confined and defined discretion, both of which are essential facets of Art. 14.[37] In another case of *Mysore vs S.R Jayaram*,[38] the Constitutional bench of the SC construed arbitrariness as opposed to the positive content in Article 14. In the landmark case of *E.P Royappa*[39], arbitrariness was formally embedded as a ground for striking down any legislative or executive action being antithetical to Article 14. The SC in *A.L. Kalra vs UOI*[40] *and D.S. Nakara v. UIO*[41] held in absolute terms that an action per se arbitrary, shall be violative of the second part of Art. 14. Thereafter, in *Ajay Hasia v. Khalid Mujib Sehravardi*[42], the Constitutional Bench of the SC held the concept of reasonableness and non-arbitrariness to be applicable even to legislative actions. In this case, the court stated that whenever there is arbitrariness in State Action, art. 14 springs into action and strikes down such State Action. Recently in *Shayara Bano v. Union of India*[43], it was held that applying the "arbitrariness doctrine", even the legislative provisions can be struck down if they are found to be discriminatory, with their operation being whimsical, excessive, unreasonable or disproportionate. Two recent judgments of the SC in *State Of T.N. v. K. Shyam Sunder*[44] *and A.P. Dairy Development Corpn. Federation v. B. Narasimha Reddy*[45] reiterated the legal position that legislative provisions can be struck down if found to be arbitrary and resultantly violative of Art. 14.

[34]Draft Digital Personal Data Protection Bill, 2022, § 19(2) (India).
[35]Diksha Bhardwaj Vinayak Das, Gupta New data Bill at odds with privacy ruling, say experts, HINDUSTAN TIMES, November 19, 2022, https://www.hindustantimes.com/cities/delhi-news/new-data-bill-at-odds-with-privacy-ruling-say-experts-101668795861038.html (Last visited on March 20, 2023)
[36]*S.G. Jaisinghani v. Union of India, AIR 1967 SC 1427.*
[37]Siddharth R. Gupta† and Kerti Sharma, and Editor, Aticle 14 and arbitrariness vis-à-vis legislative action, SCC BLOG, October 11, 2021 https://www.scconline.com/blog/post/2021/10/11/article-14-and-arbitrariness-vis-a-vis-legislative-action/ (Last visited on March 20, 2023)
[38]*Mysore v. S.R Jayaram, AIR 1968 SC 346.*
[39] *E.P. Royappa v. State of T.N., AIR 1974 SC 555.*
[40] *A.L. Kalra v. Project and Equipment Corpn. of India Ltd, AIR 1984 SC 1361.*
[41]*D.S. Nakara v. Union of India, AIR 1983 SC 130.*
[42] *Ajay Hasia v. Khalid Mujib Sehravardi, AIR 1981 SC 487.*
[43] *Shayara Bano v. UOI, (2017) 9 SCC 1.*
[44] *State Of T.N. v. K. Shyam Sunder, AIR 2011 SC 3470.*
[45] *A.P. Dairy Development Corpn. Federation v. B. Narasimha Reddy, (2011) 9 SCC 286.*

4.2 Violation of Article 21

Over the years, courts have recognized the intrinsic value of individual autonomy and the role of privacy in enabling individual autonomy and thus enjoyment and exercise of liberty and freedoms. The Right to Privacy is a fundamental right under Article 21 of the Indian Constitution. Several provisions of the impugned rules breach the Right to Privacy. As held in the *Puttaswamy case*, any restriction on this right must meet threefold requirements 1) Legality 2) Necessity and 3) Proportionality. [46] If a restriction on the Right to Privacy fails any of these requirements, it will be violative of Art. 21.

The requirement of Proportionality means that the collection of data should be the least restrictive method of achieving the goal and that there should be a balance between the extent of infringement and the importance of the goal. [47] This three-fold test mentioned above must be fulfilled for any executive action to breach the guardrails around privacy. [48] Further, Proportionality consists of four sub-components, namely- Legitimate state interest, Suitability, Necessity and Balancing. The absence of any of these components can render any interference with the right disproportionate. *Firstly,* Section 8 offers a highly diluted scheme of obtaining user consent for data processing. It presumes the consent of the Data Principal for numerous conditions laid down in sections 8(1) to 8(9). This highly vitiated scheme of consent can force greater generation and sharing of data than is necessary and entirely fails core tenets of data protection, specifically data minimisation and purpose limitation, which thus makes it a disproportionate infringement. [49]

Secondly, Section 18(3) may be used to exempt some private actors even if they process personal data which can be considered sensitive. Section 18(2) provides several situations under which the government can be exempted from the application of certain provisions of this act. [50] These blanket exemptions to the Govt. instrumentalities create the possibility of increased Surveillance from state and non-state actors, which was held to be violative of Art. 21 in *PUCL v. Union of India* [51] and most recently in *Manohar Lal Sharma v. Union of India* [52] . Further, the provisions concentrate all surveillance powers with the executive branch & do not have safeguards such as judicial review of surveillance orders in place.

---

[46] *Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.*
[47] Bhatia, supra note 28.
[48] Bhardwaj & Dasgupta, supra note 35.
[49] Singh & Kaur, supra note 29.
[50] Draft Digital Personal Data Protection Bill, 2022, § 18(2) (India).
[51] *People's Union for Civil Liberties v. Union of India & Ors., AIR 1997 SC 568.*
[52] *Manohar Lal Sharma v. UOI, 2022 SCC OnLine Del 669.*

Thirdly, Clause 18(4) exempts the "State or any instrumentality of the State" from complying with data deletion requirements under the law.[53] As a result, any data collected by the State may be retained by them forever, which again violates the Right to be Forgotten, which has been described as part of the Right to Privacy in *K.S Puttaswamy judgement* and has been affirmed by the most recent case of *Jorawer Singh Mundy* case[54]. Even in *Puttaswamy- II,* the court struck down a regulation that allowed the Unique Identification Authority of India (UIDAI) to retain certain transaction data for a period of five years. The bench noted the disproportionate nature of the provision and recognized that it affected the RTBF of citizens.[55] Also, under sec. 18, there is no clear justification given as to why the state is exempt from the storage limitation requirement. While the status of the Right to be forgotten as a standalone right is unsure, judgments such as *Vasunathan vs Registrar General* [56] had recognised it well before the Puttaswamy judgement. This right is based on the importance of the autonomy of the data principal.

5. Relevance of the New Bill in Light Of Article 19 and the Right to Information Act, 2005.

Changes to clause (j) section 8 of the RTI Act are discussed in clause 30 of the draft proposal. It recommends that this clause be changed to make it difficult for someone to obtain personal information about another person under this legislation. However, this modification is excessive in nature and is not just, fair, or reasonable. In the Puttaswamy decision, the Supreme Court declared that the right to privacy was a fundamental freedom protected by Article 21 of the constitution, but it also noted that this right was not absolute and that some reasonable limitations could be placed on it to further specific, justifiable goals, such as national security. Therefore, even though gathering a person's personal information may occasionally be necessary in order to accomplish a legitimate task, this amendment prevents us from doing so. [57]In effect, it allows the Right to Information Act to become a Right to Deny for public information officers.

As it turns out, most information sought by applicants relates to a person. This proposed amendment is the latest attempt to undermine the RTI Act,

[53]Draft Digital Personal Data Protection Bill, 2022, § 18(4) (India).
[54] *Jorawer Singh Mundy v. Union of India, W.P. (C) 3918/2020.*
[55] Verma, supra note 27.
[56]*Vasunathan v. Registrar General, 2017 SCC OnLine Kar 424.*
[57] Dalima, supra note 25.

which has made those wielding power uncomfortable because it effectively transfers power to the citizens.[58]

There are certain exceptions to the Right to Information Act. One of these, Section 8(1)(j), allows public information officers to deny requests for personal information that have no connection to public activity and which can cause an unwarranted invasion of privacy unless the applicant can demonstrate that a larger public interest justified the disclosure of such information. Section 8(1)(j) has already been widely used by public information officers to deny service records, assets, complaints and disciplinary proceedings pertaining to bureaucrats and the same was upheld in the case *Girish Deshpande vs Central Information Commission.*[59]

Instead of trying to legislatively over-rule this decision to bolster the Right to Information the government through the proposed Digital Personal Data Protection Bill, 2022[60], aims to tighten Section 8(1)(j) even further. Without a "public interest" exception, there is a concern that there will be a strong legal argument to exclude all personal information about officials, elected officials, and judges that are included in election affidavits or asset disclosure forms. They can readily claim that their fundamental right to informational privacy has been violated by being obliged to disclose their assets and income.

Because Art. 21 and 19 are interlinked, as decided in the *Rustom Cavasjee Cooper v. UOI*[61] and later substantiated by *Maneka Gandhi vs UOI,* any infringement of Art. 21, should also go through the tests of Reasonable Restriction under Art. 19(2).[62] The term “reasonable" implies intelligent care and deliberation. Legislation that arbitrarily or excessively invades the right cannot be said to contain the quality of reasonableness.

Here, under section 8 of the Act, the concept of Deemed concept allows data to be collected, stored and processed even without the express consent of an individual. Under sections 8(8) and 8(9), a range of extremely broad circumstances are mentioned, the meaning of which is open to multiple interpretations. Even for uses like ‘Credit Scoring’ (section 8(8)), which involves the use of highly personal and sensitive information, an individual’s consent can be deemed. Other phrases such as where it is reasonably expected that personal data would be provided” (section 8(1));

[58] Sailesh Gandhi, How the proposed Data Protection bill will undermine India's right to information, SCROLL.IN, November 21, 2022, https://scroll.in/article/1037879/how-the-proposed-data-protection-bill (Last visited on March 20, 2023)
[59] *Girish Deshpande v. Central Information Commission, (2013) 1 SCC 212.*
[60] Draft Digital Personal Data Protection Bill, 2022, § 18(2) (India).
[61] *Rustom Cavasjee Cooper v. UOI, AIR 1978 SC 597.*
[62] *Maneka Gandhi v. UOI, (1970) 1 SCC 248.*

"for the provision of any service or benefit to the Data Principal" (section 8(2)); "for employment," (section 8(7)); “when it is in the Public Interest” (section 8(8)); and “for any fair and reasonable purpose as may be prescribed” (section 8(9)) are susceptible to misuse.[63] These terms remain undefined and vague and thus fall out of the Reasonable restrictions under 19(2) of the constitution.

Under Sec. 18(2) of the Act, the central govt can exempt any instrumentality of the state from compliance with the law.[64] While these are legitimate concerns of the state, these terms stand undefined, and their contours are not clear in the legislation. These uncharted terminologies can lead towards surveillance for reasons that go beyond the purposes intended by the legislation. In *Chintaman Rao*[65], the SC opined that a restriction in order to be referred to as reasonable, shall not be beyond what is required in the interest of the public. Legislations which arbitrarily or excessively invade the right cannot be said to contain the quality of reasonableness. The above-mentioned expressions of the impugned provisions remain undefined and vague and thus fall out of the Reasonable restrictions under 19(2) of the constitution.

6. Conclusion

The bill, in its entirety, has put forth a complete framework for data protection. Considering the nature of the function that the bill aims to serve and the high stakes of data and its misuse, a holistic view of the bill needs to be taken. From the journey of the promotion of electronic trade through the IT Act and the subsequent steps to protect data, we have come a long way to recognising the Right to privacy as a fundamental right through the KS Puttaswamy judgement. But even with this, the need for a complete act to serve this purpose of data protection has not been fulfilled till now. Though the new attempt at this is laudable as the Digital Personal Data Protection Bill takes some major steps towards the protection of data, both the Preamble and the Explanatory Note of the Bill fail to even mention the phrase ‘Right to Privacy’.

Unlike the previous bills, ‘Non-Personal Data’ (NPD) gets no appearance and is totally out of the scope of this bill which majorly focuses on the protection of Personal Data. The removal of

Non-Personal Data from this bill is not contested as it has been widely argued that legislation controlling Personal and Non-Personal Data need not be clubbed together and both of them should be dealt with separately.

[63] Draft Digital Personal Data Protection Bill, 2022, § 8 (India).
[64] Draft Digital Personal Data Protection Bill, 2022, § 18(2) (India).
[65] *Chintaman Rao v. State of Maharashtra, AIR 1951 SC II8.*

As it seems to be a haste job, the proposed bill simply seems to progress from policy paralysis to tokenism. The word "as may be prescribed" is mentioned 18 times in the Data Protection Bill, 2022, which denies its specificity and leaves a lot of room for the Government to use its discretion from time to time for filling these gaps through delegated legislation. While the bill is praised for its clear and concise language, it is riddled with ambiguities. This ambiguity raises the possibility of undue delegation and grants the Union Government a great deal of power. The lack of detail has reduced the proposed bill to little more than the skeleton of an Act that might get passed by the Legislative body and then filled by the government's executive branches, allowing the latter additional authority to set the terms.

The concept of Deemed Consent and the Exemptions under Sections 8 and 18, respectively, is of specific concern, too. In these, the bill also outlines the exemptions and talks about how the Government can process personal data without the users' consent and store them indefinitely. The bill aims to create a Data Protection Board, ostensibly for the purpose of implementing the law on the ground, and handling complaints and breaches of the law, but is devoid of necessary independence. Subsequently, the bill outlines the exemptions and talks about how the Government can process personal data without the users' consent and store them indefinitely. Lastly, it also proposes an amendment to the RTI Act which seems misplaced since the 'information' under RTI goes beyond digital personal data.

With such palpable problems in the bill, it hardly seems to be legislation that will be able to deal with the issues of modern times. The lack of independence from the government and the ambiguities present would leave open room for interpretation that could harm the interests of the data principals. It is in this regard that there is a need to take a reformative approach and present any such exploitation of data principles. Some of the reforms could include mandating the destruction of data when the data principals give the affirmation for renewing consent cessation, establishing a sturdy mechanism to deal with the gravamen and operationalising it to deal with heavy loads of complaints, devising a mechanism to limit the definition of 'deemed consent' and holding the government liable. Apart from this, it is necessary to get a clear definition of the vague phrases used to avoid and restrict the misinterpretation of the same. As there are extensive clarifications and reforms that the bill might require, a question on the effectiveness of the bill in protecting data arises. With data of more than a billion people being affected, the stakes are high. In consonance with this, so should the protective measures be and hence in its present form, the bill seems to be deficient in enabling the same.