"DIGITAL PERSONAL DATA PROTECTION ACT" —A STRUDEL SERVED RAW!

Soumya Banerjee*

Abstract: The good news is that personal data privacy law has become a reality in India. The bad news is 95% of the public is ignorant of the same, 3% do not know what it entails and the rest 2% are voraciously engaged in an intellectual feud. Privacy as a concomitant of natural or inalienable rights has been recognized in the western hemisphere since the 18th century. In India, the legislative history of the doctrine can be traced to the trilogy of cases during the 1950's. It was only post 1978, that the apex court of the country passed a slew of judgements recognizing the right to privacy as an essential part of the right to "protection of life and personal liberty" embodied under the Indian Constitution and thereby bestowing the fundamental right status. On August 24, 2017, a nine-judge Constitution bench of the Supreme Court of India (Puttaswamy judgment) re-wrote history as it not only recognized and reconfirmed the fundamental right status of " right to privacy" but also laid the foundation of data protection law in the country. August 11, 2023, marks a historic date in the legislative annals of digital India, as the country enacted the Digital Personal Data Protection Act, 2023 ("DPDP Act" or "Act") after more than half a decade of deliberations. At a time when technology has become the defining paradigm of every business, the DPDP Act seeks to lay the foundation for developing a strong data privacy regime in the country. The Act in its new avatar is quite different from its predecessors proposed earlier. Ironically, the regulations themselves have set ajar a host of challenges, issues and steeplechases, which can barely be fathomed at this moment. In addition, the DPDP Act is yet to be notified or implemented by the Central Government. The key question this paper discusses is whether this seemingly endless period of deliberations culminated into a robust and comprehensive law or is it simply a Strudel served raw! To answer this question, the paper first charts the history of the concept with a chronological approach on a global platform. The second part of the paper charts the pre-DPDP era in India. The third part recapitulates the DPDP Act (in the present form) in a nutshell, while the fourth part dissects the DPDP Act highlighting certain potentially problematic features of this law. Lastly, the paper will examine what can be done to influence the development of a robust and sustainable data protection regime in the country in the years to come.

Keywords: Data Privacy; DPDP Act; Indian Privacy Law; Origin of Privacy Laws

* Legal Department, Yes Bank Limited, India.

Table of Contents

"You're the Apfelstrudel of mein eye"

–Chitty Chitty Bang Bang (1968)

INTRODUCTION

The good news is that personal data privacy law has become a reality in India. The bad news is 95% of the public is ignorant of the same, 3% do not know what it entails and the rest 2% are voraciously engaged in an intellectual feud. The latter two layers emerge primarily because of the different aspects involved in privacy, *viz., need, function, right, technology and legal protection.*[1] Just like a *Strudel* – a whirlpool of technique, process, and ingredients. For all those non aficionados of confectionary out there, *Strudel* is a type of sweet or savory layered pastry, where the filling is spread intermittently between layers of unleavened dough giving it a swirling pattern. Coincidentally, the oldest known strudel recipe[2] and the first ruling[3] by a Court of law recognizing the need for privacy (*though in a rudimentary form*), both find their origins in the 16th century.

August 11, 2023, marks a historic date in the legislative annals of digital India, as the country enacted the Digital Personal Data Protection Act, 2023 ("**DPDP Act"** or **"Act"**)[4] after more than half a decade of deliberations. At a time when technology has become the defining paradigm of every business, the DPDP Act seeks to lay the foundation for developing a strong data privacy regime in the country. Ironically, the regulations themselves have set ajar a host of challenges, issues and steeplechases, which can barely be fathomed at this moment. In addition, the DPDP Act is yet to be notified or implemented by the Central Government, just like a batch of freshly baked strudel resting in a rack.

The key question this paper discusses is whether this seemingly endless period of deliberations culminated into a robust and comprehensive law or is it simply a *Strudel served raw*! To answer this question, the paper first charts the history of the concept with a chronological approach on a global platform. The second part of the paper charts the pre-DPDP era in India. The third part recapitulates the DPDP Act (*in the present form*) in a nutshell, while the fourth part dissects the DPDP Act highlighting certain potentially problematic features of this law. Lastly, the paper will examine what can be done to influence the development of a robust and sustainable data protection regime in the country in the years to come.

I. ORIGINS OF THE CONCEPT CALLED "PRIVACY"

"Privacy" as a concept was alien to the early human civilization. The early homo sapiens, characterized by their bipedalism and subsistence lifestyle, largely lived in

---

[1] Karl de Leeuw and Jan Bergstra, (Eds), "The History of Information Security: A Comprehensive Handbook". Elsevier: 2007. Holvast, Jan, "History of Privacy", Holvast & Partner, Privacy Consultants, NL - Landsmeer, The Netherlands.

[2] The oldest Strudel recipe for a Millirahmstrudel, is from 1696, in a handwritten recipe at the Viennese City Library, Wiener Stadtbibliothek.

[3] *Semayne* v. *Gresham* (1604) 5 Co Rep 91; 77 ER 194 ('*Semayne's Case*').

[4] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Gazette of India, August 11, 2023.

shared common dwellings with almost no physical separation. This meant no person could escape the physical surveillance of others without special efforts [5] and consequently resulted in little or no privacy. However, as humans transitioned from being gatherers to settlers in small encampments, the first seeds of privacy were sown.

Historically, the concept of privacy can be traced to the writings of Socrates, Plato and other Greek philosophers,[6] which noticeably distinguished between the 'outer' and 'inner', 'public' and 'private'; and 'society' and solitude'. From a legal perspective, the Code of Hammurabi contained a paragraph against the intrusion into someone's home.[7] Chronological research shows that 'physical privacy' was overtly recognized in England centuries ago. According to the Electronic Privacy Information Centre, the Justices of Peace Act of 1361 provided for the arrest of peeping toms and eaves dropper. [8] The concept of privacy formally took silhouette during the colonization of North America. Hence, when a large population of the early colonists migrated to the North America from England it was not surprising that the concept also sailed along with them and they started respecting privacy (during the early 16th century), in relation to an individuals' home, family and even correspondence. Ownership and possession of the land in the vast US continent laid the foundation for the privilege of privacy. Physical privacy became the characteristic of everyday life and home became the primary place of privacy.[9] Reverberation of the same cogitate can also be seen in the famous ruling by Sir Edward Coke in the *Semayne Case [January 1604]*[10]-"*a man's home is his castle.*"

The 19th century witnessed a new series of threats which fuelled the rise of progressive regulations in the field of privacy. Preventing-copies of US census being published in public [11], unauthorized opening of mail [12], tapping into telegraph communication[13], compelling disclosure of personal information and documents[14], are some of the prominent cases in the US legal history. Then came the Warren and Brandeis publication in 1890[15], which is widely recognized as the cradle for the concept and came to be considered as the "most influential law review article of all"[16] for more than one reason. First, it highlighted the role of media [newspaper/prints] which transgressed from a mere information source to indulge in "yellow journalism". Second, the lack of common law remedy available at that time to combat such threat and lastly,

---

[5] David H. Flaherty, Privacy in Colonial New England, 2 (1972).
[6] Moore Jr., B.: Studies in Social and Cultural History. M.E. Sharpe, Inc., Armonk (1984).
[7] Solove, D. J.: *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven & London: Yale University Press, 2011. p. 4.; Lukács Adrienn: *What is Privacy? The History and Definition of Privacy*, Országos Szövetsége, Budapest, Magyarország, pp. 256-265. (2016).
[8] Holvast Jan, *History of Privacy*, Karl de Leeuw and Jan Bergstra (Eds), The History of Information Security: A Comprehensive Handbook. Elsevier, (2007).
[9] Flaherty, D.H.: Privacy in Colonial New England. University Press of Virginia, Charlottesville (1972).
[10] Court of King's Bench, All ER Rep 62, Also reported 5 Co Rep 91 a; Cro Eliz 908; Moore KB 668; Yelv 29; 77 ER 194. *Supra Note 3.*
[11] David J. Seipp, The Right to Privacy in American History, 6–7 (1978).
[12] Robert Ellis Smith, Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet, 12 (2000).
[13] *Ex parte* Brown, 72 Mo. 83, 95 (1880). See *Supra Note* 16 at 5.
[14] *Boyd* v. *United States*, U.S. Supreme Court, 616 (1886).
[15] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L.REV. 193 (1890).
[16] Harry Kalven, Jr., Privacy in Tort Law—*Were Warren and Brandeis Wrong*?, 31 L. & CONTEMP. PROBS. 326 (1966).

it advocated numerous remedies, with the principal being "an action of tort for damages in all cases"[17], for the preservation of privacy. The publication eventually led to State of New York enacting a statute[18] establishing a cause of action for invasion of privacy and subsequent introduction of statutes to safeguard against unauthorized intercepting of telegraph and telephone calls.[19]

With the dawn of the 20th century, several statutes were enacted across the world (both federal and state) and Courts vigorously recognized, reiterated, and ruled in favor of protection of privacy. Numerous statutes[20] were enacted between 1960-1980, which dealt with safeguarding privacy of individuals or their information and influenced privacy laws across the globe. The German State of Hessian[21] enacted the World's first data privacy laws at State level in September 1970, and subsequently, laid the foundation for the German Constitutional Court to recognize the fundamental right of informational self-determination[22]. In 1973, Sweeden enacted the Data Act, which is one of the first privacy laws related to computers and online activities. The next ten years in US saw rapid enactment of statutes, which aimed safeguarding the privacy of individuals against unauthorized collection[23], dissemination[24] and usage[25] of personal information *via* various communication channels.

At the international level, the United Nation ("UN") Declaration of Human Rights[26] enshrines the right to privacy under Article 12. In 1950, the European Convention of Human Rights reiterated similar protection under Article 8, subject to certain restrictions. The Organization of Economic Cooperation and Development (OECD) Privacy Guidelines [Eight Principles][27] in 1980, charts the formal birth of information privacy laws at international level. However, it was Convention 108 in 1981[28], the first binding international instrument, which aimed at protecting individuals against abuses derived from the collection and processing of personal data and sought to regulate the cross-border flow of personal data. Thereafter in 1996, the European Union promulgated the Data Protection Directive,[29] which established the basic principles for privacy legislation for EU member states and provided for a comprehensive protection of personal information, including restricting the flow of personal data outside the borders of EU. This broad-brush approach was a stark contrast to the United States' approach, which regulated privacy at a "sectoral level" in various

---

17 *Supra Note 23, 219.*
18 New York Civil Rights Law, 50–51.
19 *Supra Note 17, 157.*
20 Freedom of Information Act of 1966. Code of Fair Information Practices of 1973. Marc Rotenberg, Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), 2001 STAN. TECH. L. REV. 1, 44. Privacy Act of 1974. Foreign Intelligence Surveillance Act of 1978. Fair Credit Reporting Act of 1970. Bank Secrecy Act of 1970.
21 Data Protection Act, 1970; Datenschutzgesetz [HE 1970]. GVBl. HE 1970 S. 625.
22 Bundesverfassungsgericht. Judgement of the first senate of 15. December 1983.
23 Cable Communications Policy Act of 1984.
24 Privacy Protection Act of 1980; Video Privacy Protection Act of 1988.
25 Computer Matching and Privacy Protection Act of 1988.
26 Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (Resolution No.217A).
27 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 C (80)58/FINAL.
28 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, January 1981.
29 Council Directive 95/46, 1995 O.J. (L 281) 31–50 (EC), hereinafter "EU Data Protection Directive."

narrow contexts.[30] In 2014, the African continent adopted the Malabo Convention[31] which established the legal framework for personal data protection and cyber security with the African Union Member States, along with the mechanism for combating violation of privacy in relation to data collections, processing, transmission, storage and usage.

Between 2016-19, data privacy regulation received a big push, with the introduction of GDPR[32] and ePrivacy Regulation[33] in the European Union. GDPR became a global sensation on account of three reasons: (i) "*Brussels Effect*"[34], because of its aggressive extraterritorial scope and imposition of EU laws across the world. (ii) "*DC Effect*"[35], because of its adoption of various US data privacy innovations, e.g., privacy by design, deterrence-based fines, corporate fines and compensation from law-breaking date processors; and (iii) the "*Individual focused approach*", because of the elaborate rights it gave to individuals, e.g., right to be forgotten, object, rectifications, portability, access and notifications. In 2020, the State of California became the first US State to enact a comprehensive data privacy law, which provided certain rights to customers and paved the way for other legislation in the US (*state and federal level)*. These days, January 28 of every year is celebrated as the 'Data Privacy Day' to commemorate the date when Convention 108 was opened for signature.

II. PRIVACY LAW IN INDIA PRIOR TO DPDP ACT

Privacy as a concomitant of natural or inalienable right[36] was recognized in the western hemisphere since the 18th century. In India, the legislative history of the doctrine can be traced to the trilogy of cases (M.P. Sharma[37] - Kharak Singh[38] - Gopalan[39]) during the 1950's. Ironically, the first two judgements refused to recognize the right of privacy as a fundamental right, *in absentia* of express provisions in the Indian Constitution, while the third judgment simply assumed the existence of such rights emanating from personal liberty while subjecting it to restriction on the basis compelling public interest (based on the state test under US jurisprudence).

It was only post 1978, that the apex court of the country passed a slew of judgements recognizing the right to privacy as an essential part of the right to "protection of life and personal liberty" embodied under the Indian Constitution and

---

[30] Joel R. Reidenberg, Setting Standards for Fair Information Practices in the U.S. Private Sector, 80 IOWA L. REV. 497 (1995). Daniel J. Solove, A Brief History of Information Privacy Law, Chapter-1, 1.4.4 (2006).

[31] The African Union Convention on Cyber Security and Personal Data Protection

[32] General Data Protection Regulation, Regulation (EU) 2016/679.

[33] Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications, 2018.

[34] Anu Bradford, The Brussels Effect, 107 NW. U. L. REV. 1, 1 (2012).

[35] Michael L. Rustad and Thomas H. Koenig, Towards a Global Data Privacy Standard, 71 Fla. L. Rev. 365.

[36] American Declaration of Independence (1776); Declaration of the Rights of Man and of the Citizen (1789).

[37] *M.P. Sharma and Others* v. *Satish Chandra, District Magistrate, Delhi and Others*, 954 AIR 300, 1954 SCR 1077, AIR 1954 Supreme Court 300, 56 PUN LR 366.

[38] *Kharak Singh* v. *State of U.P. And Others*, 963 AIR 1295, 1964 SCR (1) 332, AIR 1963 Supreme Court 1295, 1963 ALL. L. J. 711, 1963 (2) CRI. L. J. 329, 1964 (1) SCR 332 1964 2 SCJ 107, 1964 2 SCJ 107.

[39] *A.K. Gopalan v. State of Madras, Union of India,* 1950 AIR 27, 1950 SCR 88, AIR 1950 Supreme Court 27, 1963 MADLW 638.

thereby bestowing the fundamental right status. The prominent cases involve impounding of passports (Maneka Gandhi[40]), telephone tapping (PUCL[41]), restrain on publication of material of a death row convict (Rajagopal[42]), inspection and search of confidential information (Canara Bank[43]), disclosure of HIV status of a patient (Mr. X v. Hospital Z[44]), medical termination of pregnancy (Suchita Srivastava[45]) and right of transgenders (NALSA[46]).

On August 24, 2017, a nine-judge Constitution bench of the Supreme Court of India (*Puttaswamy[47] judgment*) re-wrote history. The judgement not only recognized and reconfirmed the fundamental right status and reinforced the propositions laid down by above-mentioned judgments but also explicitly observed[48] that: (i) privacy is a constitutional core of human dignity; (ii) privacy safeguards personal autonomy and heterogeneity (iii) constitution must evolve with the felt necessities of time to meet the challenges thrown up in a democratic order governed by the rule of law (iv) any law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights and (v) informational privacy is a facet of the right of privacy.

Prior to the DPDP Act, there was no specific legislation on privacy and data protection in the country. Certain regulatory bodies (Telecom Regulatory Authority of India, Reserve Bank of India, Medical Council of India and Insurance Regulatory and Development Authority of India) under sector specific statutes[49] attempted to safeguard the interest of individuals by imposing restrictions on disclosure of information or documents to third parties, unless the same was required by law or the process prescribed therein. Nearly twenty-three years ago, the Information Technology Act, 2000[50] ("**IT Act**"), encapsulated provisions to protect the rights of individuals against breach of privacy by corporate entities. The IT Act was inspired by the Model Law on Electronic Commerce[51] encapsulated three elements of data protection, *viz.,* maintaining reasonable security practices and procedures to safeguard specified information classified as sensitive personal data or information which can identify a natural person ("**SPDI**"); recognition of tort remedy[52] upon breach in maintaining reasonable security practices and procedures, and lastly, the intentional disclosure of personal or sensitive information of any person, collected under a contractual relationship. The IT Act also attempted to protect the right of an individual against any unauthorized capturing, publishing, and transmission of any image of a private part of

---

40 *Maneka Gandhi* v. *Union of India* (1978) 1 SCC 248.
41 *People's Union for Civil* Liberties v. Union of India, (1997) 1 SCC 301.
42 *R. Rajagopal* v. *State of Tamil Nadu*, [(1994) 6 SCC 632; AIR 1995 SC 264.
43 *District Registrar and Collector, Hyderabad* v. *Canara Bank,* (2005) 1 SCC 496.
44 (1998) 8 SCC 296.
45 *Suchita Srivastava* v. *Chandigarh Administration*, (2009) 9 SCC 1.
46 *National Legal Services Authority* v. *Union of India*, (2014) 5 SCC 438.
47 *Justice K.S. Puttaswamy (Retd.) and Another* v. *Union of India*. (2019) 1 SCC 1.
48 *Ibid 262-265*.
49 Indian Telegraph Act, 1885; Banking Companies Act [Transfer and Acquisition of Undertakings], 1980; Credit Information Companies (Regulation) Act, 2005; Indian Medical Council Regulation, 2002; Insurance Regulatory and Development Authority of India, Regulation 2015 and 2017.
50 Act No.21 of 2000;
51 UNICITRAL Model Law on Electronic Commerce (June 12, 1996) with additional Article 5 bis as adopted in 1998.
52 Section 43A [Compensation for failure to protect data]; Ins. by Act 10 of 2009 (w.e.f. 27-10-2009).

such individual, under circumstances which violated his/her privacy[53], and thereby recognizing the sanctity of the body. In 2011, the Government introduced the Indian Data Protection Rules, which read with Section 43A of the IT Act, laid down eight rules to protect the privacy of an individual.

In July 2017, post the *Puttaswamy*[54] judgment, the Ministry of Electronics and Information Technology set-up the Srikrishna Committee[55], chaired by Justice B.N. Srikrishna (a retired judge of Supreme Court of India) to formulate the foundation of data protection norms in the country. The work of the committee formed the pedestal for the Personal Date Protection Bill of 2019[56], the first government version of the law. Unfortunately, the work of the committee and the resultant Bill of 2019 was more like saffron, white truffles and wagyu all rolled into one utopian savory strudel. Though the committee/Bill adopted a normative approach rather than US *laissez-faire* approach or the *individual dignity* centric approach adopted by EU, its expansive scope was hugely problematic, suffered from overregulation and the implementation framework more disruptive rather than transformative for the digital Indian economy. Nonetheless, it was perhaps the most comprehensive, cross-sectoral framework based on preventive requirements of business (known as "data fiduciaries") and right for individuals (known as "data principles").[57] The Bill of 2019 was withdrawn in November 2022, basis the report submitted by the Joint Parliamentary Committee, and replaced with the DPDP Bill of 2022[58]. The DPDP Bill of 2022 received the approval of the lower house (Lok Sabha) and the upper house (Rajya Sabha) in the month of August 2023 and officially became an Act after receiving the President's assent on August 11, 2023.

III. DIGITAL PERSONAL DATA PROTECTION ACT—IN A NUTSHELL

The DPDP Act comprises of 9 chapters, encompassing 44 sections and Schedule. In this part, only the key provisions of the Act have been enumerated rather than providing a narrative on the entire Act, which would have made a good case for writing a book but will surreptitiously defeat the scope and objective of this Article.

A. Applicability

The DPDP Act only applies to personal data collected from individuals, *i.e., Data Principal*[59] *in India* in a digital form or in non-digital form and digitized subsequently.[60] The Act applies to all data collected within India (*Territorial scope*) and processing of data outside the territory of India (*Extra-territorial scope*), if such processing is in connection with any activity related to offering of goods and services to Data Principal within the territory.[61] What this implies is- the Act is applicable to all individuals, who are Indian citizens, non-resident Indians and foreign citizens, if the

---

[53] *Supra Note* 60. Section 66E.
[54] *Supra Note* 58.
[55] *A Free and Fair Digital Economy, Protecting Privacy and Empowering Indians*, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, (2017).
[56] Bill No.373 of 2019.
[57] Anirudh Burman, *Understanding India's new Data Protection Law*, Carnegie India - Carnegie Endowment for International Peace, October 3, 2023; https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624.
[58] Bill No.113 of 2022.
[59] As defined in *Section 2(j)*.
[60] *Section 3(a)*.
[61] *Section 3(b)*.

data is collected in India. This extra-territorial application and scope is an unique feature of the statute (similar to the PDPA[62] of Singapore), perhaps the first of its kind in the country, which explicitly includes all individuals and permits cross-border transfer of personal data to facilitate various e-commerce websites/international businesses operating and providing goods and services in India. The Act, however, excludes personal data processed by an individual for any personal or domestic purpose or made publicly available by the Data Principal or any person who is under an obligation under any law.[63]

B. Data Processing Principles

The DPDP Act lays down the *four elements*[64] for processing any personal data, *viz*., in accordance with the provision of the Act, lawful purpose, consent of the Data Principals, and for certain legitimate uses. The terminology - '*legitimate uses*' has rechristened the concept of "*deemed consent*", which was envisaged in the draft Bill of 2022, for processing of personal data for certain special use cases without the express consent of the Data Principal. The Act, similar to the provisions under GDPR and LGPD[65], list downs the legitimates uses[66], e.g., interest of sovereignty, integrity and security of India, fulfilling the obligations under law, responding to medical emergencies involving a threat to life or health, medical treatment, occurrence of disaster and purposes of employment. What this implies is the Data Principals will not have any right to erase, correct, access their personal data, or withdraw their consent for the original purposes for which it was disclosed. At the same time, the concept will reduce the dependency of obtaining express consent in specific circumstances, and ultimately result in cost savings[67] for the businesses due to the dispensation of additional mechanisms for consent management.

C. Consent & Notice

A valid consent under the DPDP Act needs to be free, specific, informed unconditional and unambiguous in nature with a clear affirmative action.[68] What this implies is – (i) consent cannot be obtained from Data Principles on a 'deemed'[69], 'omnibus' or 'conditional' basis; (ii) consent obtained for purpose A cannot be used for purpose B, and (iii) processing of such information shall be limited only to the personal data which is necessary for the specific purposes. To simply put it, it's an opt-in model of obtaining consent *akin* to GDPR and LGPD[70]. The Act, however, does not describe the form or manner of obtaining the consent through the electronic medium, like clickwrap, two-factor authentication etc. Nonetheless, any consent provided by the Data Principal shall not be absolute or permanent. It may be withdrawn at any time,

---

62 Singapore's Personal Data Protection Act, 2021.
63 *Section 3(c) (i)(ii)*.
64 *Section 4(1), (2)*.
65 Brazilian General Data Protection Law of 2020.
66 *Section 7*.
67 Decoding the Digital Personal Data Protection Act, 2023, KPMG India, August 2023.
68 *Section 6(1)*.
69 Unless the same is exempted under *Section 7*.
70 Brazilian General Data Protection Law of 2020.

either by the Data Principal or through its Consent Manager[71] and the ease of doing so needs to be at par with the standards adopted at the time of obtaining it.

Any notice sent to the Data Principal for the purpose of obtaining consent shall specifically inform such Data Principal about the personal data, purpose for which it is processed, manner of exercising their rights and making a complaint to the Data Protection Board[72]. Every request for consent shall be presented to the Data Principal in clear and plain language, with an option to access such request either in English or any language specified in the Eighth Schedule to the Constitution, including the details of the Data Fiduciary[73] or the Data Protection Officer ("**DPO**")[74], if applicable.[75]

D. Obligation of the Data Fiduciary

The Data Fiduciary, irrespective of any agreement to the contrary or failure by the Data Principal, is solely responsible and/or liable for all compliances under the Act and Rules made thereunder, including any processing of data undertaken by itself or any Data Processor[76] on its behalf. From implementing appropriate technical measures to taking reasonable security safeguards against any breach, Data Fiduciary is the phyllo dough of the Act. Any personal data being processed by the Data Fiduciary must ensure its completeness, accuracy and consistency.[77] They are also required to erase personal data if the specified purposes is served or if the Data Principal withdraws her consent, unless the retention of such data is mandated by law.[78] Additionally, they are also responsible for establishing effective mechanism to redress the grievances of the Data Principal.[79]

E. Significant Data Fiduciary

The Act defines a significant data fiduciary ("**SDF**") as any data fiduciary or class of data fiduciaries which is notified by the Central Government basis certain factors[80] enumerated under the Act, probably on account of the following three reasons: (i) to supervise the large regulatory space intersecting numerous business organizations across diverse sectors; (ii) establishing a supervisory regime for entities of national interest and 'too big to fail'; (iii) subjecting such entities to incremental compliance requirements such as – appointment of an individual as a data protection officer ("**DPO**") based in India, appointing an independent data auditor for evaluating compliance with the Act, conducting periodic audit and data protection impact assessment, and undertaking such other measures consistent with the provisions of the Act or as may be prescribed by the Central Govt., from time to time.

---

71 As defined in *Section 2(g)*.
72 *Section 5*.
73 As defined in *Section 2(j)*.
74 As defined in *Section 2(l)*.
75 *Section 6(3)*.
76 As defined in *Section 2(k)*.
77 *Section 8(3)*.
78 *Section 7(a)*.
79 *Section 7(10)*.
80 *Section 10(1)*.

F. Processing of Personal Data of Children

The Act expressly mandates that before processing any personal data of a child or a person with disability, it shall be mandatory for the Data Fiduciary to obtain a 'verifiable consent' of the parent or lawful guardian.[81] However, the Act explicitly forbids tracking or behavioral monitoring of, and targeted advertising directed at, children or a person with disability, and processing of children's data that is likely to cause any detrimental effect upon the child.[82] Notably, the Act empowers the Central Government to exempt certain classes of data fiduciaries and processing for certain purposes from the requirement of obtaining parental consent and prohibiting behavioral monitoring. It also empowers the Central Government to exempt data fiduciaries for processing data of children above a certain age but under 18 years in certain situations without the specific obligations attached to processing children's data. What this implies is - Data Fiduciaries need to implement suitable internal mechanisms for the purpose of obtaining and collecting 'verifiable' age of the child and consent of the parent/guardian, to safeguard against any detrimental effect upon such specific class of Data Principal. Though the Act seeks to provide enhanced safeguards for the vulnerable class, the proviso clearly lacks clarity in terms of what tantamount to a 'verifiable' consent or detrimental effect.

G. Rights of the Data Principal

Chapter III of the Act enumerates certain rights of the Data Principal, which includes the right to access information about personal data[83], right to correction and erasure[84], right to grievance[85] and the right to nominate[86].Of all the rights mentioned above, the last right, *i.e.*, to nominate, assumes special significance on account of three reasons: (i) it is a unique feature of law unparallel with any privacy laws across the world which allows the Data Principal to nominate any individual in the event of death or incapacity; (ii) recognizes personal data as an perceptible and inalienable property of an individual; (iii) allows the individual to control the personal information through a nominee rather than being freely available in the public domain.

H. Cross-Border Transfer of Personal Data

Like many data privacy regulations across the world (GDPR, PIPL[87] and nFADP[88]), the DPDP Act allows free transfer of data outside the territory of India for the purpose of processing.[89] However, such transfer is subject to notification by the Central Govt. in relation the country where data may or may not be transferred.

---

[81] *Section 9*.
[82] *Section 9 (3)*.
[83] *Section 11*.
[84] *Section 12*.
[85] *Section 13*.
[86] *Section 14*.
[87] China's Personal Information Protection law, 2021.
[88] New Federal Act on Data Protection of Switzerland, 2023.
[89] *Chapter IV Section 16*.

I. Data Protection Board of India

Chapter V of the Act contemplates the establishment of a Data Protection Board ("**Board**"), a body corporate having perpetual succession and a common seal under the aegis of the Central Government. The Board is slated to be an independent body and function as a digital office with receipt of complaints, hearing, pronouncement of decision impose of penalties and adopt such techno-legal measure as may be prescribed.[90] Any appeal preferred against an order of the DPB will be required to made before the Telecom Disputes Settlement and Appellate Tribunal ("**TDSAT**") established under the Telecom Regulatory Authority of India Act, 1997. Any appeal against the order of the TDSAT will be preferred before the Supreme Court of India. Two significant provisions deserve special attention here- (i) Board may accept from a person facing action for non-observance under the law, voluntary undertaking in respect of any matter related to the observance of any provisions of the Act at any stage of the proceedings before the Board.[91] (ii) Central Govt. has the power to call for information from the Board or Data Fiduciary and authorize blocking of access to the public which enables the Data Fiduciary to carry out activity in India.[92]

J. Jurisdiction of the Board and Penalties

The Board is subsumed with all the powers of a Civil Court and bars the jurisdiction of any other Civil Court in the country from entertaining any proceedings or granting any specific reliefs, which the Board is empowered under the Act, or any rights exercised by it thereof. The Board is also empowered to impose monetary penalties to the extent of INR 250 Crores, after the adjudication of any matter, after considering seven factors[93] enumerated under the Act.

IV. A HALF-BAKED STRUDEL

According to Auguste Escoffier, School of Culinary Arts, a successful baker is one who, *amongst* other qualities, understands the importance of "*mise en place*", communicates clearly and gives attention to details. Any attempt to cut corners, or a haphazard approach can lead to subpar results. A legal framework is no different. The efficacy of any statute largely depends upon four factors - the legislative approach which is reflected in the provisos and figuratively forms '*mise en place*' of the ensuing law; clarity and precision; flexible yet predictable and one which inspires public trust and legitimacy. Deviate from the said recipe and one is bound to end up with a law, which is no better than a soggy strudel.

Unfortunately, close scrutiny of the Act reveals the deep fault lines it hides within and the host of challenges, issues and implications, which can barely be fathomed at this moment. Following is some of the challenges and issues.

A. Flawed Legislative Approach

In the words of Chief Justice Dr. D.Y. Chandrachud, the formulation of a data privacy framework is a complex exercise which needs to be undertaken by the State

---

[90] *Section 28*.
[91] *Section 32*.
[92] *Section 37*.
[93] *Section 33(2)*.

after a careful balancing the privacy concern and legitimate state interest.[94] The Act though is not a reflection of such a thought process. While the US legislators followed the '*laissez*-faire' approach, EU followed the comprehensive data governance approach, and some Asian countries like Singapore and Japan adopted the '*disparate approach*'; Indian legislatures have adopted an '*interventionist approach'*. The fundamental flaw of such an approach lies in the fact that it not only undermines the theory of separation of power[95] and the delegation doctrine[96] but also prone to the following risks – (i) the legislature tends to delegate the "*essential legislative powers"* under the garb of delegated legislation; (ii) lacks legislative policy; and (iii) the executive branch tends to usurp the legislative powers. The DPDP Act is a classic example of this fallacy, as the Central Government has been granted wide discretionary powers without adequate legislative policy or standards under the Act, e.g. notifications of significant Data Fiduciary[97], processing of personal data by the State or its instrumentalities,[98] processing of personal data of children,[99] non-application of certain provisions under the Act to certain Data Fiduciary or class of Data Fiduciaries[100], establishment of the Board, composition and appointment of members [101], and power to call for information and issue directions.[102] By failing to set essential and clear legal policy on a whole range of issues, as mentioned above, the DPDP Act simply transforms the Executive into the primary lawmaker on multiple counts. This approach of the Central Govt. not only undermines the role played by the Legislature in the country but also casts a dark shadow on the aspiration and trust reposed on the State by billions of people in the country.

B. Allied Laws

DPDP Act is being hailed as the first cross sectoral law in the country. In reality, it is a disguised '*laissez*-faire' approach as evidenced by Section 38 of the Act which prescribes that the *Act shall be an addition to and not in derogation of any other law for the time being in force*. What it implies is that instead of having an overarching effect it encourages grandfathering of existing laws across multiple sectors. The dichotomy gains prominence considering that the DPDP Act has a direct impact on about 50[103] different laws in the country, and many of such laws govern - (i) a specific sector (e.g. Information Technology, Taxation, Health, Defense, Labor, Corporate and Financial), (ii) have independent regulators and mechanisms (e.g. Reserve Bank of India ("**RBI"**), Insurance Regulatory and Development Authority in India ("**IRDA**"), Telecom Regulatory Authority of India ("**TRAI**"), Employees Provident Fund Organization ("**EPFO**") etc.; (iii) have different objective of collecting data; (iv) have specific parameters for data collection and storage; and (v) have different adjudication and grievance mechanisms. This will obviously lead to ambiguities and inconsistencies in the way data is collected, processed, stored, safeguards and rights of the data principles and breaches adjudicated in future. While the Act attempts to amend some

---

94 *Supra Note* 58.
95 *Ram Jawaya* vs. *State of Punjab*, A.I.R. 1955 SC 549.
96 *In re The Delhi Laws Act, 1912, The…* vs. *The Part C States (Laws) Act, 1950,* A.I.R 1951 SC 332.
97 *Section 10*.
98 *Section 17(2)(a)*.
99 *Section 9(5)*.
100 *Section 17(5)*.
101 *Section 18*.
102 *Section 36 and 37*.
103 *Annexure- C, Supra note* 66.

glaring inconsistencies in about four statutes[104], but it is a long way before any uniformity or cohesiveness is achieved across sectors, if at all it is achieved or meant to achieve.

C. Applicability

The DPDP Act aptly encapsulates both territorial and extra-territorial jurisdiction to protect the data of the Data Principal. However, where it falters is the imbedded ambiguity under the Act and lack of a forward-looking approach. As discussed earlier, the Act is applicable to all individuals, who may be Indian citizens, non-resident Indians and foreign citizens, if the data is collected in India. This may pose a peculiar problem, if the individual was an EU or a New Zealand citizen, where on account of their home country laws, more than one State may exercise jurisdiction over any matter, invoke conflict of laws, and Courts will be left to determine which State has a more 'substantial connection' to the issue at hand and thereby exercise jurisdiction. Secondly, the extra-territorial application is subject to the caveat that the processing is in connection with 'activity related to the offering of goods and services to Data Principals within the territory of India'. Exercise of this prescriptive jurisdiction is predominantly based on the principle of territoriality rather than passive personality. This is a narrow application of the concept of extra-territoriality and a stark departure from most of the privacy laws across the world, e.g. GDPR, PIPL, LGPD, PDPA etc., that seeks to protect the data of individuals within their territory, irrespective of where the collection and processing is done and devoid of any such caveats, as stipulated under the Act. Thirdly, the DPDP Act adopts a traditional approach (i.e. activity related to the offering of goods and services) in its application and abjectly overlooks activities like analyzing, profiling and evaluating behavior and activities of the individuals, which is the new information gold mine. Fourthly, though the Act does not have a retrospective effect, its applicability, without any existing legislative policy or safeguards, is bound to have retrospective implication or obligations upon Data Fiduciaries across various sectors. What it implies is any processing (from mere storage and indexing to complicated analysis) of personal data, irrespective of when it might have been collected, will be within the ambit of the Act. E.g. The DPDP Act may be applicable to a bank which may be collected personal data 20 years ago from a customer for the purpose of account opening and the account is still active today. Lastly, considering the cross-sectoral applicability, the legislature has adopted a transitional approach in the DPDP Act. This approach is intended to bridge the gap between the commencement of the Act and its operation prior to it, with the objective of having a smooth transition over time from the existing laws. Unfortunately, this approach attracts a *Staling* effect. Just like a batch of freshly baked strudel loses its freshness due to retrogradation of starch molecules, inclusion of multiple transitional clauses in the Act is also likely to cause severe chaos and confusion leading to multiple litigations. This will impair effective implementation of the Act and be more disruptive than contemplated by the legislature. Consequences of similar approach being adopted in some in some the recent Indian statutes, e.g. The Insolvency and Bankruptcy Code[105] and Goods and Service Tax[106], is clear evidence of such proposition.

---

[104] *Section 44*.
[105] Act 31 of 2016.
[106] Act 12 of 2017.

D. Government—the Unregulated Hand

The DPDP Act, despite its patent objective, has been quintessentially curated as a powerful tool in the Government's armory. State and its instrumentalities have been completely kept outside the purview of the Act, in the interest of sovereignty, integrity, national security, relation with foreign states, maintenance of public order, prevention of cognizable offences[107], research, archival and statistical purpose[108]. This wide category will ensure that the Government has complete autonomy in the collection, processing, usage and storage of personal data. Currently, public entities and Government agencies hold personal information for a majority section of society. This seriously puts a dent on the transparency and trust factor, as Government excessiveness cannot be ruled out. This is a stark departure from some of the privacy laws enacted across the world e.g. GDPR, NZPA[109], PDPL[110], that encourages transparency and accountability for all Data Fiduciaries, irrespective of whether public or private sector. Secondly, the Act empowers the Government to make 'Rules"[111] for all or any aspect of the privacy laws. Unlike countries like US, UK and Australia, which have overarching legislation regulating the framing of subordinate legislation, India has none. This gives unfettered rights to the Government to alter the design of the statute itself. Thirdly, Government has been provided wide discretionary and unguided rule-making powers with respect to granting exemptions[112] under the Act, without any legislative policy or safeguards, whatsoever. This again grants wide unfettered right to the Govt. which is prone to political will, bias, and misuse. Lastly, the Govt. has complete control over the functioning of the Board, including but not limited to, the composition, appointment, terms of employment and salary of the Chairperson/Members, manner of reporting breaches to the Board and techno-legal measure to be adopted. In essence, the invisible and unregulated hand of the Govt. will control and govern the complete functioning and outcome of the Board as the Act simpliciter reduces it to a mere extended arm of the Government.

E. Data—the Modern Gold

What apple is to an *apfelstrudel*, data is to privacy laws. The DPDP Act adopts a broad-brush approach and provides for an inclusionary definition of 'personal data',[113] without any exhaustive or indicative list, of what is, will or may be considered as a personal data. This pertinent question has perhaps been left at the discretion of the Board or under the wide 'rulemaking' authority of the Government. Whatever the reasons are, the Act faulters on this aspect on multiple counts. Firstly, the definition lacks reference to '*unique identifiers*'[114], as reflected in many foreign privacy

---

[107] *Section 17(2)(a)*.
[108] *Section 17(2)(b)*.
[109] Privacy Act, New Zealand, 2020.
[110] Personal Date Protection Law, Saudi Arabia, Issued pursuant to Royal decree No. (M/19) dated 16/09/2021
[111] *Section 40*.
[112] *Section 17(3), Section 17(5), Section 9(5).*
[113] *Section 2(t)*.
[114] California Consumer Privacy Act of 2018, effective 1/1/2024 – AB 947 and AB 1194 updates posted to cppa.ca.gov April 2024. Pursuant to definition (aj) of CCPA- "Unique identifier" or "unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias;

legislations (e.g. CCPA[115], PDPA, PIPA[116]) which constitutes the forage for marketing and solicitation activities across sectors. In absence of unique identifiers, marketing tools operating on unique IDs and cookies such as analytics platforms and customer data platforms may be successful in circumventing the law. Secondly, lack of identifiers would mean exclusion of quasi-identifiers as well, which when combined with other identifiers can render greater harm to an individual. Latanya Sweeny in her work has shown that neither gender, birthdates or postal codes uniquely identify an individual but when combined can sufficiently identify 87% of individuals in the US.[117] Thirdly and most importantly, the Act neither defines 'sensitive personal data' nor provides a segregation from aforesaid definition. 'Sensitive personal data' like biometric, financial or health data, passwords, religion etc., has been expressly defined and included under multiple privacy legislations across the world (e.g. CCPA, CPPA, PIPL, NFADP, PDPL, PDPA, PIPA etc.), owing to enhanced security requirement, active consent requirement (as envisaged under GDPR and LGP) and right to limit the usage of such data. In short, the Act neither defines sensitive data nor puts any kind of incremental obligations upon Data Fiduciaries or Processors, to safeguard the interest and privacy of the individuals the Act proclaims to protect.

F. Consent

Consent has been viewed as an expression of an individual's autonomy or control, which has the consequence of allowing another person to legally disclaim the liability for acts which has been consented to.[118] Notice coupled with choice which culminates into a consent, forms the very foundation of the consent philosophy on which the DPDP Act has been constructed. While countries across the globe are adopting a right-based approach ('Opt-in/opt-out') to privacy laws (e.g. CPPA, LGPD, PDPA) Indian legislatures are still stuck to the traditional approach. Sadly, this consent-based approach is outdated in the wake of internet, AI, and change in technology. The different elements[119] (free, specific, informed, unconditional, unambiguous with a clear affirmative action, specified purpose for processing) of consent stipulated under the Act fades away on account of the following: (i) absence of consent standards for online or digital collection, use and disclosure of personal information; (ii) absence of model notices to demonstrate compliance with the Act; (iii) discretion of the Data Fiduciary to obtain consent in any form or manner, leads to inherent weakness (e.g. pre-ticked checkboxes, notice not provided prior to processing) which are fairly common in the Indian market; (iv) lack of informed consent (e.g. non-disclosure of consequences of collection, use and disclosure of personal information or name of third parties with whom such information is shared); Secondly, this approach will invariably lead to

---

telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.

115 *Supra Note 127.*

116 Personal Information Protection Act, South Korea, Act No. 19234, March 14, 2023.

117 L. Sweeney, *"Simple Demographics Often Identify People Uniquely",* Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.

118 Adam Moore, Toward Informational Privacy Rights, 44 San Diego Law Review (2007) at p. 812; Anita L. Allen, Why privacy isn't everything: Feminist reflections on personal accountability (Rowman & Littlefield, 2003) at pp. 115-16; John Kleinig, The Nature of Consent in The Ethics of Consent- Theory and Practice (Alan Wertheimer and Franklin Miller (eds.), Oxford University Press, 2009) at p. 4.

119 *Section 6(1)*.

consent fatigue (apart from dampening user experience) for the Data Principal, in absence of a consolidated and supervised consent dashboards or platforms, which are seamlessly integrated with consent manager or tag managers. Thirdly, one of the crucial elements overlooked (intentionally or inadvertently) in the Act is the relationship between consent and contractual necessity. Both the ingredients needed to be de-coupled, as any consent to processing extracted by holding contractual rights hostage tantamount to consent being treated as 'not' free.[120]. Surprisingly, the Act does not include contractual necessity under 'Legitimate uses'[121] and it has been left to the Government, Board or Courts to clarify whether businesses can enforce contract under the aforesaid Section or will it again be required to obtain explicit consent for processing of personal data.

G. Non-Consensual Processing

Any free and fair normative privacy framework is dependent on two factors, i.e., autonomy of individual vis-à-vis national, social, and economic interest. The DPDP Act which rechristened the concept of 'deemed consent' (introduced under the Bill of 2022), as "Certain legitimate Uses"[122] has completely dislodged this fine balance. Firstly, the Act places the State and its instrumentalities on a lower pedestal as compared to private entities, especially in relation to processing data on a non-consensual basis. It includes scenario, where consent has *either* been previously provided[123] or no-consent has been provided at all[124]. This wide exception is bound to raise several interpretational issues e.g. nature of entity performing the function, nature of the function itself and the extent of usage of such data. Secondly, the legitimacy of collection and usage of such data will be opaque, considering that the State and its instrumentalities are empowered to formulate the policy under delegated legislation, in absence of any specific provision in the Act. Thirdly, no thought has been given to data minimization, purpose limitation and transparency, as suggested by the Supreme Court of India in the *Puttaswamy Judgment*. On the contrary, State excessiveness will be prone to occur in lieu of the consideration (subsidy, benefits, services, permits etc.) promised to the Data Principal. Lastly, the so called 'legitimate uses' lacks any sort of safeguards to protect the interest of the Data Principals. E.g. usage of data for employment purposes should be invoked only when it involves a disproportionate or unreasonable effort on the part of the employer to obtain a valid consent.

H. Data Fiduciary

Data Fiduciary plays a pivotal role in any privacy law considering the dual objective it seeks to fulfil, i.e., collection, usage, and storage of data *vis-à-vis* the accomplishment of the purpose desired by the Data Principal. The DPDP Act, while encompassing most of the obligations envisaged under the 2019 Bill, lacks the comprehensiveness and finesse, to shape India's digital landscape in the 21st century. One of the foremost issues is the absence of obligation to ensure fair and reasonable processing by the Data Fiduciary to prevent abuse of power. Fair[125] and reasonable processing implies two elements, i.e., obligation to uphold the best interest of the Data

---

120 Recital 3, GDPR.
121 *Section 7*.
122 *Supra Note 134.*
123 *Section 7(b)(i)*.
124 *Section 7(b)(ii)*.
125 UK GDPR, Article 5(1)(a); Recital 39 GDPR.

Principal and the processing is not beyond the expectation of the Data Principal.[126] Secondly, the Act lacks explicit provisions for data minimization when compared to privacy laws[127] across the globe. The data limitation principle forms the bedrock of any privacy laws[128] as it ensures that the data collected is limited to what is necessary to achieve the primary purpose and if such collected data is no longer necessary for such purpose, it ought to be destroyed. Unfortunately, in absence of any explicit provision under the Act, the Data Fiduciary is under no such express obligation and thereby increasing the chances of abuse of power. This risk attains a larger magnitude and leads to tangible harm to individuals with the emergence of Big Data, processing vast amount of data at scale to discern patterns of individual patterns and market trend.[129] Thirdly, the Act does stress on the transparency principle. Mere obligation on the Data Fiduciary to give notice to the Data Principal at the time of collection is highly inadequate. Additionally, the obligation to inform the Data Principal of the basis of processing, legal obligation for such processing, persons with whom the data is shared, and period of retention is entirely absent. Lastly, the Act does not deal with the principle of storage limitation, which ought to have obligated the Data Fiduciary to delete or anonymize the personal data after the purpose is achieved. This essentially exposes the personal data to theft, copying, transferring or usage, without any kind restriction or consequences upon the Data Fiduciary.

I. Missing Ingredients of the Act

The DPDP Act has, consciously or otherwise, watered down various provisions which were incorporated in the Bill of 2019. Some prominent provisions need a special mention here. The Act entirely excludes offline personal data and data collected through non-automated processing from within its purview. Data portability[130], which enables the Data Principal to receive structured format of the collected data and transfer it to a different institution has been completely discarded. While the Bill of 2019 proposed deanonymization as a criminal offence, the Act has completely de-criminalized all offences. Concept like 'Right to be forgotten" has been outrightly junked considering competing State rights and interests. Complete autonomy has been bestowed upon the Government (without any requirement to consult or seek guidance from the Board) in deciding and notifying the countries where personal data may be transferred for the purpose of processing. The 'harm' caused on account of processing the data, including the obligations on the Data Fiduciary to mitigate such harm or the right of the Data Principal to seek compensation for such harm are entirely missing in the Act. Lastly, the Act encompasses various generic words without suitable explanations or standards, leaving it for the Government, Board, or the Courts to define, interpret and implement the same. E.g. "detrimental effect",[131] "well-being of the child"[132], or "verifiably safe".[133]

---

126 *Supra Note 66.*
127 UK GDPR, Article 5(1)(c); Recital 39 GDPR, PDPL.
128 GDPR, FIPPs, OECD Guidelines on the Protection of Privacy and Transborder flow of Personal Data (2013).
129 White Paper of the Committee of Experts on a Data Protection Framework for India, 2018, at p. 8.
130 Incorporated in various privacy laws. E.g. CDPA, LGPD, PIPA.
131 *Section 9(2)*.
132 *Ibid*.
133 *Section 9(5)*.

J. A Toothless Board

What a good baking instrument is to a strudel, a robust enforcement mechanism is to a good law. Compromise on the instrument and the result will be a streusel and not a strudel. The DPDP Act suffers from this major lacuna, as the Board (in comparison to DPA-its proposed predecessors) has been reduced from a sector-agnostic, independent and comprehensive regulatory body to a procedural body merely for the purpose of overseeing data breaches, direct remedial measures and conduct inquires. Firstly, the independence of the Board has been seriously compromised given that the selection and appointment of the Chairpersons/members, their tenure, salary, allowances, and functioning are exclusively decided by the Central Government[134] and not by a specialized committee. No transparent pre-requisite regarding the professional qualification, expertise or experiences have been prescribed. Secondly, the possibility of conflict-of-interest situations, arising vis-à-vis the Chairpersons/members and their functioning cannot be ruled out in absence of a clear demarcation on the powers and functionality coupled with the complete discretion available with the Chairperson under the aegis of the Central Government. Thirdly, the Board does not have any regulatory tools like formulation of best practices code, issuance of guidance or public statements. All is at the behest of the Central Government. Lastly, the Board ought to have been the independent regulator exercising powers across the sectors in the Indian economy. Unfortunately, the Board has a subordinate status to the various sectoral regulators, which will seriously undermine the entire privacy framework and enforcement mechanism. To sum up, the Board is a toothless tiger under the tutelage of the Government, which will be incapable of protecting the interest of the Data Principal, both in letter and in spirit.

K. Dysfunctional Dispute Resolution Mechanism

One of the gaping drawbacks under the Act, is empowering TDSAT[135], an existing tribunal to discharge the functions of the appellate tribunal under the Act. TDSAT, a twenty-four-year-old tribunal, is already the appellate tribunal for telecommunications, cable services, broadcasting, cyber and airports related disputes. It is saddled with 5426 pending cases[136] (approx. 50% of the total disposed cases[137] since inception) as on date. Hence, it is highly improbable that TDSAT will render effective and speedy adjudication mechanism. Secondly, the TDSAT comprises of members who have no or little technical expertise, know-how or experience in the field of information technology, cyber, internet laws, AI or such related fields. Hence, to think that TDSAT will have any meaningful impact or adjudication role under the Act is extremely farfetched by any yardstick.

L. Technologically Agnostic

Technology and privacy, quantitively speaking, are inversely proportional to each other, in terms of growth, implication, risk and protection. Hence, privacy laws of

---

[134] *Section 19, 20, 22, 27(3)*.

[135] Telecom Disputes Settlement and Appellate Tribunal established under the Telecom Regulatory Authority of India Act, 1997.

[136] Statistical Report of Pending Cases (2024), available at: https://tdsat.gov.in/Delhi/services/pending_report.php.

[137] Total Cases-11280. Statistical Report of Disposed Cases (2024), available at: https://tdsat.gov.in/Delhi/services/disposal_report.php.

the 21st century need to have a harmonic relationship with technology. Unfortunately, the DPDP Act does nothing in this context. Firstly, biometrics and genetic data, which includes fingerprints, retina, voice and facial patterns and genetic code have not been provided enhanced security, safety and storage safeguards unlike privacy laws of many countries[138]. Secondly, surveillance mechanisms engaged by the State and private entities, e.g. CCTVs, and GPS, and enhanced technological features like night camera, motion detection and computer assisted operations, are completely outside the realm of the Act. Thirdly, the Act does little to address the issues arising out of Data mining and Internet, especially considering the tremendous amount of data which is collected, stored and processed without the consent and knowledge of the users. E.g. Cookies coupled with spam and spyware facilitate the collection and analysis of personal information leading to identification of individuals, without the user even realizing or knowing the consequences of it. Lastly, the Act is extremely ill equipped to handle some of the future technologies like ambient technology, neurolinguistics and grid technology, as these complex technologies are capable of not only collection and monitoring of personal information of the user but also effecting changes in behavioral and neural patterns, choices and responses of such users.

V. TOWARDS A ROBUST AND SUSTAINABLE FRAMEWORK

Considering that the DPDP Act has been enacted after nearly 81 amendments since it was first tabled before Parliament in 2019, a complete overhaul now may not be possible or advisable at this time. Hence, it is felt that to achieve a robust and sustainable privacy framework within the ambit of the Act, the following 14-point recommendations needs to be considered to meet the aspirations of digital India and its 1.5 billion inhabitants:

1) The Central Government should extend the application of Act to cover processing of all data pertaining to individuals within the Indian territory, irrespective of where the collection and processing is done or whether the Data Processor is established or whether such Data Processor is providing goods and services in India. Additionally, all analyzing, profiling and evaluating behavior and activities of the individuals, should be brought within the ambit of data processing.

2) To minimize the effects of transitional approach of the Act, the Central Government needs to provide comprehensive Rules and specific timelines for its implementation, in consultation with sectoral regulators and stakeholders.

3) To minimize the effect of consent fatigues for the Data Principles, the Central Government must provide or facilitate Consent frameworks, consent dashboard and data trust score for Data Fiduciaries, operated by public or regulated entities.

4) The Central Government should formulate prescriptive rules related to consent from Data Principals, especially in connection with consent

[138] GDPR, CPRA, nFADP, PDPL.

managers and children's data, by stipulating models forms and dynamic consent renewals and withdrawals.

5) The Central Government should formulate rules and guidelines on collecting, usage and storage of sensitive data and corresponding enhanced obligations upon data fiduciaries. Opt-in rights and express consent must be made mandatory.

6) The Central Government should formulate adequate Rules to protect "Big Data" processing by Data Processors based on collection and purpose principles. Perhaps usage of blockchain technology can be considered in this context.

7) The Central Government along with the sectoral regulators should formulate rules and guidelines on data portability and interoperability, especially in sectors facing increasing digitization e.g. banking, insurance and social media. Introduction of hybrid and multi-cloud strategies coupled with uniform terminology and standards for data portability and interoperability, will go a long way to mitigate the risks arising from such activities.

8) The Central Government should formulate rules and guidelines related to the usage of surveillance cameras, workplace surveillance, outsourcing services and direct mailing by Data Fiduciaries or Data Processors.

9) To avoid multiple litigations and disputes related to data privacy issues and breaches by the State and its instrumentalities, the Central Government must formulate and implement a grievance mechanism for Data Principles in the country.

10) The Central Government in consultation with sectoral regulators/experts should frame and promulgate rules, code of best practices, policies and advisory related to data discovery, data mapping, loss prevention, data erasure and recovery.

11) The Central Government and Board should encourage, and facilitate usage of privacy enhancing technologies (PETs) e.g. secure multiparty computation, differential privacy computing and on-device analytics, in addition to the existing technologies like encryption, and tokenization, across sectors.

12) Specialized bench should be constituted under TDSAT, consisting of tecno-legal experts from various sectors. The functioning of the Bench should be on a 'fast-track' basis and equipped with modern technology to ensure live streaming of proceedings, digital filings, recordings and proceedings, 24x7x365 accessibility. Additionally, powers may include appointment of amicus curia and technical experts, pre-mediation process, disclosure requirements and fixed timelines for expediating the disposal of cases.

13) The Board should enter into formal arrangements or MoU with sectoral regulators to lay out a uniform and comprehensive plan or framework for the implementation of the Act, including addressing critical elements of the privacy laws, e.g. form and manner in which personal information is collected, stored and used, breaches and grievance mechanism.

14) Sector regulators and industry bodies, e.g. Indian Bank's Association (IBA) for banking, should formulate comprehensive plan or framework for the implementation of the Act, to avoid information and implementation asymmetry within the respective sectors.

CONCLUSION

Given the deep fault lines in the Act, as demonstrated above, it will be interesting to see how and when the Act is implemented, Rules promogulated and its comprehensiveness to design the privacy framework for digital India. The regulatory architecture and the institutional framework that will crystallize over the next few years will decide how well (or not) personal data privacy is safeguarded. The new law provides for the dough but is clearly far away from a *de jure* data privacy law. Lastly, considering the '*interventionist approach'* adopted by the Government, the success of the Act will vastly depend upon the political will, intention and proactiveness of the government machinery. Until then the DPDP Act is simply a strudel served raw!