ALLIANCE UNIVERSITY
Private University established in Karnataka State by Act No.34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi
Alliance School of Law

International Journal
of Law and Social Sciences (IJLS)
Volume 10, Issue 1, 2024
Print ISSN: 2454-8553, Online ISSN: 2583-8644

A NEW AGE OF DATA PRIVACY LAWS IN INDIA: REVIEW OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Subhajit Saha[1], *Surjashis Mukhopadhyay*[2]

DOI: https://doi.org/10.60143/ijls.v10.i1.2024.114

Abstract

Having been duly sanctioned from both the Houses of the Parliament of India, the "Digital Personal Data Protection Bill" was formally enacted by the President of India on August 11, 2023. After deliberations and debates spanning over 2 years, the Digital Personal Data Protection Act 2023 stands as the outcome of the fifth iteration of the proposed personal data protection legislation.

As India's first-ever cyber-privacy Act, it is designed to protect all Indians' personal data. The enactment marks a significant milestone by establishing a devoted legal framework in the country. It draws attention to the significance of the Indian Data Protection Board, its main features, and the responsibilities and rights of both individuals and organizations. Non-personal data is not covered by the DPDP Act, which is focused on digital personal data. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data of Information) Rules, 2011 and Section 43A of the Information Technology Act, 2000 will be superseded by the DPDP Act 2023 - once its provisions come into effect.

The Act is applicable to the treatment of digital personal data in India regardless of whether the data is digitised after being collected offline or online. If such processing is done outside of India in order to supply services or products in India, it will also be covered. Only with an individual's consent and for a legitimate reason personal data can be handled. Certain lawful uses, such as an individual's voluntary data sharing or the State's processing of data for licences, permits, benefits, and services, may not require consent. Data Fiduciaries will have a duty to ensure data accuracy, store data securely, and remove it after it has served its purpose.

Keywords: Data Protection, Data Privacy, Data Principal, Data Fiduciary, Digital Personal Data Protection Act 2023.

Introduction

Since the inception of the independence of the nation, India has always been a face, a poster child of the democratic and republic countries of the Asia-Pacific rim. India has been a pioneer of legal activism, human rights, good governance, fundamental rights, law and legacy. But for generations, since the time of framing of the Constitution, the topic of the right to privacy has been left on a thread. In times of the pre-internet era, the problems with breaches of privacy have not been a matter of grave concern. So, the legislature has let the privacy laws remain unchanged until 2023 when the Parliament took a significant leap of faith for the data privacy laws in passing the Digital Personal Data Protection Act, 2023 in both the Houses of the Parliament[3].

India and Privacy - A Sociological Approach

India is a diverse nation with a huge population. India is a melting pot of diversity to the world. It has pro-

1. Student of Law, BA LLB (Hons), Department of Law, University of Calcutta, West Bengal.
2. Student of Law, Surendranath Law College, University of Calcutta, West Bengal.
3. Bareh, C.K., *Reviewing the Privacy Implications of India's Digital Personal Data Protection Act 2023 from Library Contexts*, DESIDOC Journal of Library & Information Technology, 44(1) (2024).

moted the idea of being a secular state since the time of independence and included the word 'secular' in the Preamble of the Constitution during the time of emergency. India is a peace-loving country situated in a peninsular region surrounded by many neighbouring states amongst which some have developed clashes throughout the chronology of the historical scroll. Despite being troubled with breaches of the national security and espionage of some of the enemy states, India has come a long way from choosing violence and dominion. To understand the nature of the Indian Sovereign State, one must explore the history of the nation in brief. India has always been welcoming of change and newness. From the time of the Persian invasion back in 550 BCE to the European invasion in the 18th century to the British Raj till 1947, India has been welcoming of change and novelty to their culture, heritage and societal norms. As a result, civilisation has been carved out by time, cultural paradoxes, amalgamation of morals and etiquette, pacifism and a thrust for survival through age and time. Indian cultures and morals are thus a significant reflection of the social contract theory where the family is the organism which survives on its own if social order is let to remain unchanged. In such cultural upbringing, one tends to be with the one, the true organism that survives on its own, i.e society. Thus, people remaining open to criticisms and constructivism have most of the time kept their personal affairs, but their credentials, rather open and public. Despite being open to the world, the world extended its arm to people through an enclosed society where one's limitation of their belonging to the society is geography, views and language. As a result, a breach of privacy was not a question of concern where a wrong step or a step towards righteousness was highly debated, thought about, decisive and discussed with experts[4]. But for the past few decades in this overview of the social contract, the society has disintegrated with the nuclearisation of families, financial sufficiency of the members of the now disintegrated organism, and impulsiveness of individuals while making decisions without discussing repercussions. The nuclearisation of families has caused the breaking of the family system to a far more minute one which has caused a search for employment opportunities by units of the pre-disintegrating organism. This has resulted in the rise of minute authoritative units of the neo-family structure where one is the master of his own will. Thus, came secrecy and an age of isolation where the openness is dismal. This is how the societal order of the neo-Indian social contract has created a want to keep affairs, which are personal, private and lives undisturbed from the crowd of the rat race.

The Need for Privacy Laws

Although the Right to Privacy is implied in the Constitution of India, it does not expressly mention the safeguards for the right to privacy in Part III of the Constitution. Part III consists of the fundamental rights and is considered the 'Magna Carta' of the Constitution. Supreme Court of India has traced the origin of the right to privacy from Part III of the Constitution and a nine-judge bench in Justice K S Puttaswamy v Union of India 2017 laid down that the right to privacy has been guaranteed in the Constitution of India and traced from several rights including Article 21 which embodies the right to life and personal liberty.

Before the DPDP Act, 2023 the need for India's very own segment of privacy laws was too meagre. The conception of privacy was pinpointed to a very concise area - credentials as in data related to name, financial stability, banking data, transactional history, etc. - before the emergence of the internet in India. For the pre-internet era in India, a set of legislations were introduced in various pre-existing Indian statutes namely the Information Technology Act (2000), Indian Penal Code (1860), Indian Evidence Act (1872), and Code of Criminal Procedure (1973). The statutes introduced via various amendments did not include much introspection on data protection and remedies to data breaches. With a huge shift in the organisation, documentation and analysis of official operations and a huge shift of private individuals and enterprises towards a reliance on digitalization, a need for strict and resilient privacy laws emerged. India's digital landscape has witnessed exponential growth over the years, with the number of Internet users surpassing 560 million and projected to reach over 650 million by 2023. However, this growth also underscores a stark reality: approximately half of India's population still lacks access to the Internet. Despite this digital divide, the Indian government has been proactive in implementing various digital initia-

4. Dubey, S., *A Comparative Analysis of Data Privacy Laws across India, EU and USA*. Journal of Legal Studies & Research, 10(1), 52-64 (2024).

tives under the National e-Governance Plan (NeGP) since 2006. These initiatives span across sectors such as agriculture, healthcare, education, and finance, aiming to enhance governance and service delivery. However, alongside the rapid digitisation, concerns about data privacy and security have become increasingly prominent[5].

A Rise of Digital Governance, Privacy Breaches and Cybersecurity Challenges

Under the National e-Governance Plan (NeGP), India has embarked on a journey of digital transformation, introducing numerous initiatives to streamline government services and improve citizen engagement. These initiatives include the implementation of projects like Aadhaar, the Open Government Data (OGD) platform, Sugamya Bharat Abhiyaan, and the BHIM app, among others. While these endeavours have undoubtedly enhanced accessibility and convenience for citizens, they have also led to the generation of vast amounts of data, raising concerns about privacy breaches and data misuse.

In spite of the benefits offered by the age of digitalisation, India has grappled with significant privacy breaches and cybersecurity challenges.[6] As per the reports, India has ranked third globally in the field of data breaches, with millions of users affected. These breaches revolve around various personal data, including names, phone numbers, addresses, passwords, and unique identification numbers, which are often exploited for illicit purposes. Notable examples of data breaches in India include the Air India data breach, the leakage of CAT 2020 exam results, and COVID-19 test data leaks from government websites. Such incidents have underscored an urgent need for robust data protection measures for safeguarding privacy rights of the citizens.

Enactment of the Digital Personal Data Protection Act (DPDP), 2023

Recognising the need to address privacy concerns in the era of digitalisation, the Indian Parliament enacted the Digital Personal Data Protection Act (DPDP) in August 2023. This legislation aims to regulate the collecting, processing and sharing of personal data by government entities and private enterprises simultaneously. The DPDP Act represents a significant step towards safeguarding data privacy and ensuring security for Indian citizens amidst the expeditiously evolving digital landscape. The enactment of the DPDP Act has had implications for both government agencies and private businesses operating in India's digital ecosystem. Government entities are now required to adhere to strict data protection standards ensuring the confidentiality and integrity of citizens' personal information. Similarly private enterprises, including e-commerce platforms and online vendors, must comply with the provisions of the DPDP Act for safeguarding customer data and preventing unauthorised access and misuse. India's journey towards digital transformation[7] has been highlighted by remarkable progress and unprecedented challenges. While digital initiatives have revolutionised governance and service delivery, they have also raised concerns regarding data privacy and cybersecurity[8]. The enactment of the Digital Personal Data Protection Act (DPDP) in 2023 represents a imperious milestone in addressing these concerns and safeguarding citizens' privacy rights. Moving forward, both government and businesses need to prioritise data protection and adopt vigorous security measures to ensure a safe and secure digital environment for all.

Overview of the Statute

The Digital Personal Data Protection Act, 2023 of India is the first ever act to protect the personal data of its citizens. Influenced by the European General Data Protection Right (GDPR), the Act deals with articulate

5. Srinivasan, S., Sinha, V. and Modi, S., *Drafting a pro-antitrust and data protection regulatory framework,* Indian Public Policy Review, *4* (5 (Sep-Oct), 35-56 (2023).
6. Dhiman, S. and Singh, S., *Cybercrime and Computer Forensics in Epoch of Artificial Intelligence in India*, Cyber Law Reporter, 2(4), 13-32 (2023).
7. Awasthi, P., Ganapati, S. and Tai, K.T., *Digital transformation in a large democracy: the case of India,* Asia Pacific Journal of Public Administration 1-34 (2024).
8. Raza, M.A., *Cyber Security and Data Privacy in the Era of E-Governance*, Social Science Journal for Advanced Research, 4(1), 5-9 (2024).

data protection against data breaches and cybercrimes,[9] fine and punishments for violation of data protection outside or inside the territory of India via enhancement of reasonable security practices and procedures for handling personal information (PI) and sensitive personal data or information (SPDI) as mentioned in section 43A of the Information Technology (IT) Act, 2000 and Information Technology Rules, 2011. Some privacy principles can be traced out from the coverage of the Act throughout its nine chapters and one schedule. Some of the principles which can be drawn as a summary of the efficiency of the DPDP Act, 2023 are:

1. Data Collection and Notice
2. Data Retention
3. Data Processing
4. Data Sharing
5. Users' Consent
6. Users' Right
7. Users' Security
8. Children's Data
9. Compensation

Data Fiduciary

Section 2(i) of the Digital Personal Data Protection Act, 2023 defines 'Data Fiduciary' as 'any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data'. Hence, Data Fiduciary stands related to the principles of data collection, notice and users' consent over data collection of the said users. 'Data processor'[10] on the other hand means any person who processes personal data of a Data Principal on behalf of a Data Fiduciary. Before the DPDP Act, 2023 there was no robust privacy regulation on collection and recording of personal data other than section 43A of the IT Act, 2000.

Section 4 of the DPDP Act deals with the third principle stated in the aforementioned list of principles and states accordingly the grounds for processing personal data which are – "a person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose[11] for which the Data Principal has given consent or for certain legitimate uses."[12]

The DPDP Act, 2023 talks about the obligations of Data Fiduciary in its second chapter. Of those obligations, section 5 and 6 speaks for some specific obligations. Section 5(1) of the DPDP Act, 2023 specifically states that the Data Fiduciary, while requesting the Data Principal for consent, is obligated to serve the Data Principal with a notice pertaining to the information as to why the personal data of the Data Principal is proposed to be processed, to the manner in which the Data Principal may exercise rights relating to consent as mentioned in section 6 and 13 of the Act, the manner in which the Data Principal may make a complaint to the Board of Data protection, as mentioned in Section 18 of the Act, in such manner and as may be prescribed[13].

Where the Data Principal has given consent to the Data Fiduciary is obliged to give a notice. Again Section 6 of the DPDP Act, 2023 deals with consent of the Data Principal and the Data Fiduciary's obligation to ask for the said consent and every request for that consent must be presented to the Data Principal in clear terms, making the data principal understand, in English or any language specified in the Constitution. Additionally, contact details of a Data Protection Officer has to be provided for communication regarding the Data Principal's rights. If personal data processing depends upon the Data Principal's consent, the Data Principal has the right to withdraw it at any time. The Data Principal bears the consequences of withdrawing consent, but this action does not affect the legality of processing personal data based on consent obtained before withdrawal. Upon withdrawal of consent by the Data Prin-

9. Oberoi, N. and Mehra, N., *Navigating India's Data Protection Landscape: A Brief Overview and Actionable Insights*, Cyber Law Reporter, 2(4), 53-63 (2023).
10. Section 2(k) of the Digital Personal Data Protection Act, 2023.
11. Section 4(2) of the Digital Personal Data Protection Act, 2023: "For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law."
12. Section 4(1) of the Digital Personal Data Protection Act, 2023.
13. Mukhija, K. and Jaiswal, S., *Digital Personal Data Protection Act 2023 in Light of the European Union's GDPR*, Jus Corpus LJ, 4, 638 (2023).

cipal, the Data Fiduciary must, with immediate effect, cease processing their personal data, unless the law permits a processing without consent. The Data Principal is entitled to a Consent Manager designated for the management of specified consent of the said Data Principal and the Consent Manager acts on behalf of the Data Principal and is also accountable to them. The Consent Manager is obligated to hold onto prescribed obligations and be registered with the Board, as mentioned in Section 2(c), under specified conditions. In case of any dispute relating to the consent given by the Data Principal for processing of the personal data, the Data Fiduciary is obligated to provide evidence concerning the fact that a proper notice was given and an undivided consent was obtained in accordance with the Act.

The Data Fiduciary is bound to follow the general obligations placed upon it under section 8 of the DPDP Act, 2023. A Data Fiduciary shall be responsible to comply with the provisions of DPDP Act, 2023 and the rules made thereunder in respect of any processing undertaken by the Data Fiduciary or Data Processor on its behalf. The Data Fiduciary can utilise a Data Processor to handle personal data on its behalf, particularly for activities related to offering goods and services to the Data Principal, under a valid contract. When processing personal data that may impact the Data Principal or be shared with another party, the Data Fiduciary must ensure the accuracy, completeness, and consistency of that data. To comply with the DPDP Act of 2023, the Data Fiduciary must implement suitable technical and organisational measures. It is required to safeguard personal data in its possession or under its control, including data processed by a data processor, by employing reasonable security measures to prevent breaches. In the event of a breach, the Data Fiduciary must notify the board, and affected data principals in a manner so prescribed. Unless data retention is necessary according to the Act, the Data Fiduciary must erase personal data upon the Data Principal's withdrawal of consent or when the specified purpose no longer applies, and ensure the Data Processor also erases any relevant data. Additionally, the Data Fiduciary must disclose the contact information of a data protection officer and establish an effective grievance redress mechanism for Data Principals.

Section 9 of the DPDP Act, 2023 sets out a set of stringent obligations of the Data Fiduciaries in case of processing of personal data of children. Section 9 states that 'before processing any personal data of a child or a person with disability who has a lawful guardian', the data fiduciary is duty bound to obtain a verifiable consent of the parent of the child or lawful guardian. A Data fiduciary should not undertake processing of any personal data which can cause an adverse effect on the well-being of a child.

Section 2(z) of the DPDP Act, 2023 introduces the concept of a significant data fiduciary, determined by the Central Government based on factors such as the amount and sensitivity of personal data processed, risks to data principal rights, impact on India's sovereignty and integrity, risks to electoral democracy, security of the state, and public order. These factors guide whether an ordinary data fiduciary can be designated as a significant data fiduciary. Section 10(1) empowers the Central Government to make this designation through notification. Section 10(2) outlines the additional obligations of a significant data fiduciary, including appointing a Data Protection Officer based in India to handle grievances, an independent Data Auditor for audits, and conducting periodic Data Protection Impact Assessments and audits.

Data Principal

The Digital Personal Data Protection Act of 2023 introduces the concept of a Data Principal, representing consumers in the handling of their private information. According to Section 2(j) of the DPDP Act, 2023, a Data Principal is defined as the individual to whom the personal data pertains. This includes children, with their parents or legal guardians, and individuals with disabilities, along with their lawful guardians acting on their behalf. A Data Fiduciary relies on the explicit and relevant consent of the Data Principal. Without a Data Principal, a Data Fiduciary cannot operate unless prescribed or exempted by law, in accordance with the provisions of this Act.

Chapter III of the Digital Personal Data Protection Act, 2023 outlines the rights and responsibilities of a Data Principal across sections 11 to 15. Sections 11 to 14 detail the rights of a Data Principal as per the Act, while Section 15 specifically addresses the duties or responsibilities of a Data Fiduciary.

Section 11 of the Act outlines the Data Principal's entitlement to access personal data information. Accord-

ing to subsection (1), the Data Principal holds the right to receive from the Data Fiduciary a summary of their personal data under processing, along with the identities of all other Data Fiduciaries and Data Processors with whom such data has been shared. Additionally, any relevant information regarding the personal data and its processing must be provided, subject to the Data Principal's prior consent to the Data Fiduciary. However, subsection (2) of Section 11 introduces an exception to this right. It states that if a Data Fiduciary shares the Data Principal's personal data with another Data Fiduciary authorised by law to access such data, the Data Principal is not entitled to access personal data as described in clauses (a) and (b) of Section 11(1).

Section 12 of the DPDP Act, 2023 addresses the right to correction and erasure of personal data. Subsection (1) specifies that a Data Principal has the right to request correction, erasure, updating, or completion of their personal data, provided they previously consented to the Data Fiduciary. Subsection (2) outlines the Data Fiduciary's responsibility to rectify inaccurate or misleading personal data, complete incomplete data, and update information upon receiving a request from the Data Principal.

An exception lies to this right in sub-section (3) of this section where it says that 'the Data Fiduciary shall erase the personal data of the Data Principal on request, unless retention of the same is necessary for a specified purpose in compliance with any law.'

Section 13 of the DPDP Act, 2023 grants the Data Principal the right to utilise a grievance redressal mechanism offered by a Data Fiduciary or Consent Manager for addressing concerns regarding their personal data or the exercise of their rights under the Act. According to subsection (1), the Data Fiduciary or Consent Manager is required to address grievances within a timeframe specified by regulations. Before escalating the matter to the Board, the Data Principal must attempt to resolve the issue through this internal grievance redressal process[14].

Right to nomination is the fourth and final right awarded to the Data Principal within section 14 of this Act. It states that a Data Principal is entitled to designate another individual, as specified by regulations, to act on their behalf if they die or become incapacitated[15]. In this context the said "incapacity"[16] refers to the inability of exercising the Data Principal's rights under the Act or its rules due to mental incapacity or physical infirmity.

With completion of the discussion about the rights of a Data Principal, and a coverage of the ambits of the principles namely users' consent, users' rights, and users' security, the discussion regarding the duties and liabilities of the Data Principal remains due. Section 15 in Chapter III of the Digital Personal Data Protection Act, 2023 enshrines the duties of the Data Principal. The section specifies that when exercising rights under this Act, a Data Principal must adhere to all current applicable laws. Additionally, they must not impersonate another individual when providing personal data, must not withhold any important information when submitting personal data for official documents, and must refrain from submitting false or frivolous complaints to a Data Fiduciary or the Board. Furthermore, when exercising the right to correction or erasure, they should only provide information that is authentic and verifiable.

Data Protection Board

The Digital Personal Data Protection Act, 2023 for the first time ever introduces the idea of establishing a data protection board in section

2. Section 2(c) defines 'Board' as 'the data protection board of India established by the Central Government of India'. Section 18 of this Act lays down the procedure for the establishment of the data protection board which states that 'for the purpose of the Act, there shall be a board established and to be called the data protection board of India with effect from such date as the central government of India may appoint by notification'. The Act also expressly states that the Board should be a corporate body established by the name of 'Data protection Board of India' with a headquarter at a place as notified by the Central government. By having

14. Sundara, K. and Narendran, N., *Protecting Digital Personal Data in India in 2023: Is the lite approach, the right approach?,* Computer Law Review International, 24(1), 9-16 (2023).
15. Section 14(1) of the DPDP Act, 2023.
16. Section 14 sub-section (2) of the DPDP Act, 2023.

a perpetual succession and a common seal, the Board also has the power to hold, acquire and dispose of both a movable and immovable property, and to contract by the name of 'Data Protection Board of India' and also has the power to sue or be sued. Section 19 states that a chairperson of the board should be appointed by the central government after assessing that he is a person of ability, integrity and standing who has special knowledge or possesses practical experience in 'the fields of data, governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy law, regulation or techno regulation'.

Chapter VI of the Digital Personal Data Protection Act, 2023 has provided some powers and functions of the board in Section 27 and some procedures that have to be followed by the board in Section 28. The powers and functions vide Section 27 are as follows –

1. It is the duty of the board to respond to the personal data breaches by urgently guiding remedial actions with the conduction of inquiries, imposition of penalties and investigation of complaints from the Data Principals concerning the breaches of their personal data or the breaches of the obligations of Data Fiduciaries who are duty bound to protect the interest of Data Principal from a breach of private data. Again, the board is obligated to investigate the breaches of the Consent Manager registration conditions and impose penalties and investigate the breaches of any intermediary obligations under section 37(2) upon being referred from the Central Government and imposing the penalties justly.
2. The Board is also at discretion to issue necessary directions after having given the concerned party one opportunity to be heard and having recorded the reasons, to ensure compliance with the act, in writing. The Board is an independent body when it comes to primary operations relating to digital capacity. It can also independently manage complaints, hearings and decide digitally on receiving complaints, references and directions while utilising technological measures as outlined in section 27(1) of this Act. The board also is bound to take necessary actions while following its rules responsible for assessing the grounds for initiation of an enquiry. The Board may either stop proceedings if insufficient grounds exist with reasonable documentations or ensure the enquiry in strict compliance with this Act and adherence to principles of natural justice if sufficient grounds are found. The board possesses powers similar to the Civil Courts under the Code of Civil Procedure, 1908. It can summon any individual under oath and accept evidence.

Methods and Materials

The Digital Personal Data Protection Act, 2023 (DPDPA) marks a significant turning point for India, ushering in a new era of data privacy rights for its citizens. This Act establishes a comprehensive framework to govern the collection, processing, storage, and transfer of personal data in the digital realm. The enactment of this signifies a watershed moment for India, heralding a new era of robust data privacy protections for its citizens. This legislation establishes a comprehensive framework governing the collection, processing, storage, and transfer of personal data within the digital domain. The methods and materials that underpin this transformative legal instrument are:

The DPDP Act, 2023 imposes several important obligations on data fiduciaries, which are entities that determine the purpose and means of processing personal data. A breakdown of some key obligations are:

Methodological Framework

Consent and Transparency

The DPDPA emphasises informed, freely given, and verifiable consent as the bedrock of data privacy. Data fiduciaries (organisations processing personal data) must demonstrably obtain consent before processing any individual's data. This consent needs to be explicit, purpose-specific, and obtained through mechanisms that ensure genuine understanding from the data principal. The Act prescribes specific requirements for obtaining valid consent, guaranteeing that individuals are well-informed about how their data will be used.

Valid Consent: Data fiduciaries can only process personal data based on freely given, informed, and specific consent from the data principal (the individual whose data is being processed) [Section 4]. The Act outlines

specific requirements for obtaining verifiable consent [Section 6].

Notice: Data fiduciaries must provide clear and accessible notices to data principals about the data being collected, the purpose of processing, and their rights under the Act [Section 5].

Data Security and Breach Management

The Digital Personal Data Protection Act, 2023 ensures and safeguards the security of personal data through –

1. Security Safeguards: The Act mandates data fiduciaries to implement reasonable security safeguards to prevent data breaches. This includes measures to protect against unauthorised access, disclosure, alteration, or destruction of personal data [Section 8(5)].
2. Data Breach Notification: In the event of a data breach, data fiduciaries are obligated to inform the Data Protection Board and affected individuals in a prescribed manner and timeframe [Section 8(6)].

Data Processing and Accountability

The Act establishes a robust framework for accountability, placing the onus on data fiduciaries to demonstrably comply with its provisions. This includes appointing a data protection officer and implementing comprehensive data governance practices.

1. Accuracy and Completion: Data fiduciaries must make reasonable efforts to ensure the accuracy and completeness of the personal data they hold [Section 8(1)(a)].
2. Data Minimization: The Act promotes data minimization, requiring data fiduciaries to collect only the personal data necessary for the specified purpose [Section 7].

Data Processing Agreement

When using data processors (third-party service providers) to handle personal data, data fiduciaries must enter into written agreements outlining the processor's responsibilities and ensuring compliance with the Act [Section 8(2)].

Individual Rights and Grievance Redressal

1. Right to Access and Correction: Data fiduciaries must provide individuals with the right to access their personal data and request corrections if inaccurate [Section 10].
2. ii. Right to Erasure and Portability: Individuals have the "right to be forgotten" and can request data deletion upon fulfilling its purpose [Section 18]. Additionally, they can request data portability to transfer their information to another service provider [Section 19].
3. Grievance Redressal Mechanism: The Act mandates data fiduciaries to establish a grievance redressal mechanism to address user complaints regarding data handling practices efficiently [Section 20].

Materials Supporting Digital Data Protection Act, 2023

The effectiveness of the DPDPA hinges on several key materials that provide further guidance and support for its implementation:

The Act Itself: The Act serves as the primary legal document outlining the principles, provisions, and obligations related to data privacy.

Regulatory Framework: The government is expected to develop regulations that will provide further details on specific aspects of the Act. These may include the manner of obtaining consent, data security standards, and procedures for handling data breaches. These regulations will flesh out the framework established by the Act and provide practical guidance for stakeholders.

Data Protection Authority Guidelines: The data protection authority is likely to issue guidelines on various aspects of the Act, offering practical guidance to data fiduciaries and individuals alike. These guidelines can address frequently asked questions, clarify ambiguities, and promote consistent implementation across different sectors.

Judicial Precedent: Court interpretations of the Act and related cases will play a crucial role in shaping how the data privacy landscape evolves in India. As the Act is implemented, legal challenges are likely to emerge, and court rulings will provide clarity on the interpreta-

tion of specific provisions. This will contribute to the ongoing development of data privacy jurisprudence in India.

The DPDPA represents a significant leap forward for data privacy in India. However, its implementation will be a dynamic process. Here are some key considerations for the future:

Capacity Building Initiatives: Data fiduciaries will need to adapt their practices to comply with the Act's requirements. This may involve investments in technology, staff training, and developing robust data governance frameworks. Capacity building initiatives by the government and industry associations can play a crucial role in ensuring smooth implementation.

Public Awareness Campaigns: Raising awareness among individuals about their data privacy rights and how to exercise them is essential for the Act's effectiveness.

Result and Discussion

As data becomes increasingly central to all-around business and personal affairs, robust mechanisms to address grievances and disputes related to data protection are essential. The construction of an appellate tribunal under the DPDP Act 2023 is a critical qua de novo component in ensuring that the rights of individuals and entities are protected effectively.

Under the Digital Personal Data Protection Act, 2023, the constituted appellate tribunal plays a pivotal role in ensuring the efficacy and fairness of India's data protection regime. By providing an independent, specialised, and speedy avenue for appeals, the tribunal helps uphold data principals' rights while simultaneously ensuring data fiduciaries' accountability. It is obvious that for the tribunal to realise its full-fledged potential, it must be adequately resourced, accessible, and well-integrated within the broader judicial framework. As India navigates the complexities of data protection in the digital age, the appellate tribunal will undoubtedly be a cornerstone of the legal landscape, safeguarding the delicate balance between privacy and innovation.

As a necessary corollary to the right of grievance redressal as granted to a Data Principal by Section 13 of this Act, Chapter VII of the statute directs an opportunity toward the concerned disputants on the novel as well as noble Alternative Dispute Resolution processes. The most prominent of such processes is probably the utilisation of a party-nominated mediator vis-a-vis mutual agreement.

General Structure of Furnishing Appeals

1. **Initial Grievance Redressal**: Data Principals can first raise their grievances with the Data Fiduciary, i.e., the entity collecting or processing the data. If the response from the Data Fiduciary is unsatisfactory, the Data Principal can approach the Data Protection Board of India (DPBI).
2. **Appeal to the Appellate Tribunal:** If a party is aggrieved by an order/directive of the DPBI, they have the right to appeal to the Data Protection Appellate Tribunal. This tribunal serves as an independent body to review and rectify the decisions made by the DPBI[17].
3. **Further Appeals:** Decisions of the Appellate Tribunal can be further appealed to the High Court (thereby, attracting Section 18 of Telecom Regulatory Authority of India Act, 1997) ensuring a multi-layered review process that upholds justice and fairness.

The infringing entity may provide the Data Protection Board of India with a voluntary commitment (or a mutually amended version of the same) about future compliance, including publicly stated guarantees related to action or inactivity in this regard. Such undertakings will be a bar to further actions once they are approved. On the other hand, the assuring entity's failure to follow the requirements of the undertaking will be considered a breach Ipso facto. Section 32(5) provides that in such a case, the Board may, after giving such a person a chance to be heard, proceed as per the provisions of Section 33.

If the Data Principal feels that the DPBI's decisions or directives are unfair, they have the right to submit an appeal to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) within 60 days of the receipt of the order in question together with the necessary fees, as stated in Section 29(2). The TDSAT's judgement must be rendered within six months, which is then

17. Section 29 of the DPDP Act, 2023.

appealable to the Supreme Court of India. In dealing with any such appeal, Section 29(8) mandates that "the Appellate Tribunal takes prudence so as to not cause prejudice to the sacrosanct provisions of Section 14A and Section 16 of the Telecom Regulatory Authority of India Act, 1997". It is worth mentioning in this context that the TDSAT, much like the DPBI, is designed to act as a virtual office with appellate capabilities akin to those of civil courts of law. Furthermore, under Section 30(1), while the TDSAT's proceedings and conclusions are 'digital by design', it retains the ability to issue the orders passed by it as formal decrees. Regardless, the TDSAT may send such directives to a local civil court for enforcement as stated in sub-Section (2) of Section 30.

Importance of Appellate Tribunal

1. **Ensuring Fairness and Accountability:** The Appellate Tribunal provides an independent platform for reviewing decisions made by the DPA. This independence is vital for ensuring that decisions are fair, unbiased, and accountable. The Tribunal operates in a transparent and considerably public-friendly manner. An example of such responsible conduct is embodied in Section 29(7) stating, "Where any appeal under S. 29(6) could not be disposed of within the period of six months, the Appellate Tribunal shall record its reasons in writing for not disposing of the appeal within that period."
2. **360-Degrees Justice:** The streamlined and intensive mechanism for appeals to ensure that decisions made by the Data Protection Authority can be challenged and reviewed with much ease and pace. This infallibly maintains checks and balances within the data protection framework.
3. **Preventing Arbitrary Decisions:** The possibility of appealing decisions ensures that the DPA's actions are subject to scrutiny. This prevents arbitrary or unjust decisions, promoting a culture of transparency and accountability within the data protection regime.
4. **Specialised Expertise:** The tribunal is expected to comprise individuals with expertise in data protection laws, cyber-technology, and ancillary fields. This adroit knowledge plus practical experience is essential for making informed decisions on complex data protection issues.
5. **Enhancing Faith:** By providing a transparent and sure-fire mechanism for appeals, the tribunal helps in building trust among Data Principals and Fiduciaries. Knowing that there is a reliable system to address grievances can increase compliance and respect for the law.
6. **Speedy Resolution:** The tribunal aims to provide a quicker resolution to disputes compared to traditional courts, which is essential given the fast-paced nature of data-related issues. This can help in the timely redressal of grievances, thereby enhancing trust and confidence in the data protection framework.

Challenges and their Consideration

1. **Capacity and Resources:** Ensuring that the tribunal is adequately resourced and staffed is critical. Without sufficient capacity, the tribunal could face delays, undermining its effectiveness. Besides, as a matter of capacity development, establishing mechanisms to monitor and evaluate the effectiveness of ADR processes is crucial. This includes tracking outcomes, ensuring compliance with procedural standards, and continuously improving the system based on feedback. While maintaining confidentiality, the ADR process must also be transparent enough to build trust among stakeholders. Discovering the optimum equilibrium between transparency and privacy is a complex challenge.
2. **Asymmetrical Power Dynamic:** Data Principals, often simpletons, may lack the legal or technical expertise to effectively represent themselves in ADR proceedings, whereas Data Fiduciaries, statistically most of whom are firms and corporations, typically have access to extensive legal resources. In many cases, there is a significant power imbalance between Data Principals and Data Fiduciaries, especially large corporations. Ensuring that ADR processes are fair and do not disproportionately favour more powerful entities is essential.
3. **Awareness and Accessibility:** It is important that data principals are aware of their rights to appeal and that the process is accessible. This includes

making sure that the procedures are straightforward and not overly burdensome. For ADR to be genuinely effective, it must be accessible to all parties involved, including those from rural or less technologically advanced areas. Ensuring that the ADR process is user-friendly and accessible to individuals with varying levels of digital or media literacy is a significant challenge, especially in the context of a demography like India.

4. **Integration with the Judicial System:** The appellate tribunal must effectively integrate with the broader judicial mainframe. This includes ensuring that there is clarity on the jurisdiction and the relationship between the tribunal and higher courts. The decisions made through ADR must be recognized and upheld by the judicial system to prevent parties from circumventing the process through subsequent litigation. But there are presently silos in the framework in this regard. The ADR mechanism under the DPDPA must be harmonised with existing legal frameworks and judicial processes to prevent conflict with other legal provisions. A clear pathway is needed for integrating ADR outcomes into the broader legal system.

5. **Competence:** Given the technical nature of many data protection issues, the tribunal must stay updated with technological advancements to make informed decisions. Creating and maintaining an effective ADR mechanism requires substantial resources, including trained mediators and arbitrators who are knowledgeable about both data protection laws and the technical aspects of data processing. Finding and training such experts is complex. Moreover, ADR decisions may be inconsistent across different cases and jurisdictions. Measures must be adopted to maintain the credibility and reliability of the ADR mechanism.

6. **Legal Lacunae:** Many scholars have speculated that the DPDP Act is not exhaustive in terms of determining its impact on Dispute Resolution processes or any other legal proceeding conducted online or through other digital platforms. For instance, Commercial Arbitration Proceedings include a large amount of sensitive material, which has a significant risk of being misused. Thus, certain guidelines are necessary to deal with such vulnerable data and the necessity to maintain their confidentiality within the scope of the statute.

Conclusion

The Digital Personal Data Protection Act, 2023 represents a landmark step in India's legislative framework for data protection. Peers and pundits alike have touted this law as a contemporary disruption in the country's burgeoning ecosystem of Information and Communications Technology; particularly, the cybersecurity sphere. It aims to provide panoptic safeguards for personal data, chaperone data influx-efflux elasticity, regulate data processing activities, and establish mechanisms for enforcement and redressal. DPDP Act suffices as the quintessential blueprint on which future de facto data privacy will crystallise. The success of the DPDP Act 2023 will largely depend on its effective implementation, ability, and flexibility to equitably balance regulation with innovation; the potency of the Data Protection Authority; and the quality of commitment of the Government, on whom substantive discretionary powers have been vested. All in all, the law definitely serves as a progressive catalyst for India's digital socio-economy to ascend past its nascent stature.

References

1. Awasthi, P., Ganapati, S. and Tai, K.T., *Digital transformation in a large democracy: the case of India*, Asia Pacific Journal of Public Administration 1-34 (2024).
2. Bareh, C.K., *Reviewing the Privacy Implications of India's Digital Personal Data Protection Act 2023 from Library Contexts*, DESIDOC Journal of Library & Information Technology, 44(1) (2024).
3. Dhiman, S. and Singh, S., *Cybercrime and Computer Forensics in Epoch of Artificial Intelligence in India*. Cyber Law Reporter, 2(4), 13-32 (2023).
4. Dubey, S., *A Comparative Analysis of Data Privacy Laws across India, EU and USA*. Journal of Legal Studies & Research, 10(1), 52-64 (2024).
5. Mukhija, K. and Jaiswal, S., *Digital Personal Data Protection Act 2023 in Light of the European Union's GDPR*, Jus Corpus LJ, 4, 638 (2023).
6. Oberoi, N. and Mehra, N., *Navigating India's Data Protection Landscape: A Brief Overview and Actionable Insights*, Cyber Law Reporter, 2(4), 53-63 (2023).

7. Raza, M.A., *Cyber Security and Data Privacy in the Era of E-Governance*, Social Science Journal for Advanced Research, 4(1), 5-9 (2024).
8. Section 14 sub-section (2) of the DPDP Act, 2023.
9. Section 14(1) of the DPDP Act, 2023.
10. Section 2(k) of the Digital Personal Data Protection Act, 2023.
11. Section 29 of the DPDP Act, 2023.
12. Section 4(1) of the Digital Personal Data Protection Act, 2023.
13. Section 4(2) of the Digital Personal Data Protection Act, 2023: "For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law."
14. Srinivasan, S., Sinha, V. and Modi, S., Drafting a pro-antitrust and data protection regulatory framework, Indian Public Policy Review, 4(5 (Sep-Oct), 35-56 (2023).
15. Sundara, K. and Narendran, N., *Protecting Digital Personal Data in India in 2023: Is the lite approach, the right approach?*, Computer Law Review International, 24(1), 9-16 (2023).