A Detailed Analysis of

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 [DPDPA 2023]

Part 1 – Overview of the DPDPA 2023

Mr. M. G. Kodandaram, IRS.
Assistant Director (Retd)
ADVOCATE and CONSULTANT

After an extensive quest to establish a law safeguarding the personal data and privacy rights of Indian citizens, the Indian Parliament has unveiled a groundbreaking legislation known as 'The Digital Personal Data Protection Act, 2023', often abbreviated as 'DPDPA 2023'. This Act marks a significant milestone in the realm of digital data protection. It is meticulously crafted to regulate the processing of digital personal data, striking a delicate balance between acknowledging individuals' rights to protect their personal information, and addressing the legitimate needs of organizations (fiduciaries) to lawfully process such data. The DPDPA 2023 provides a structured legal framework for the collection, storage, and utilization of personal data while equipping individuals with rights and remedies in cases of data breaches or violations.

The Act is structured into nine chapters, encompassing 44 sections, each dedicated to addressing various facets of digital personal data protection and regulation. This article series is divided into multiple parts, each offering an in-depth exploration of different aspects of the Act. In Part 1, we present an overview of the DPDPA 2023, laying the foundation for a comprehensive understanding of this pivotal piece of legislation. In the subsequent parts of this series, we will dissect each chapter and section in detail, providing insights and analysis to help you navigate the complexities of the DPDPA 2023.

PRIVACY in Democratic Cyber World

In the modern world, democracy and the protection of fundamental rights are cornerstone of civilized societies. Among these fundamental rights, the right to personal privacy, which has been held to be inevitable part of the right to life, enshrined in Article 21 of the Indian Constitution, is a beacon of hope for every citizen. Article 21 states, "*No person shall be deprived of his life or personal liberty except according to procedure established by law*." This simple yet profound statement underscores the significance of safeguarding an individual's life and personal liberty from any arbitrary encroachment by the state. It means that every citizen, regardless of their background or circumstances, has the right to live and be free, subject only to procedures defined by the law.

Privacy, a foundation of personal liberty, stands as a fundamental right upheld by democratic nations worldwide. It forms an inseparable part of an individual's right to lead a life with dignity and is often encapsulated as the 'right to be left alone'. This

crucial notion transcends borders and encapsulates as a universal principle proclaimed in the Universal Declaration of Human Rights back in 1948. In essence, personal privacy signifies the capacity to manage one's personal information and to exist without unjustified scrutiny or invasion into one's private life. In democratic values, privacy assumes a place of paramount significance. It serves as a protective shield against the encroachment of individual freedoms by external entities, whether they be governmental or private. This shield is not solely a matter of convenience, but a fundamental aspect of human honour and autonomy.

In the era of digital transformation, the concept of privacy has evolved into a multifaceted and paramount concern. In the wake of an unprecedented data deluge, propelled by the omnipresence of the internet and rapid technological progress, the notion of individual privacy has seamlessly extended its domain into the digital realm. Citizens have become "Netizens," in the digital world. The internet is often referred to as the "global commons," a space open for participation by all and accessible to the entire population. India has emerged as a major outsourcing destination for digital data processing. This trend offers greater economic efficiency and has allowed for the proliferation of intangible assets that provide extreme mobility. Added to this, the cloud technology has revolutionized data storage, enabling individuals and organizations to store vast amounts of data remotely. The borderless nature of the digital landscape has raised apprehensions about privacy and security. The digital world, by its nature, respects no national boundaries.

The cyber society offers enormous potential for anonymity to its members. It has been aptly described as "the world's biggest copy machine," where information can be easily duplicated and disseminated. This presents both opportunities and challenges. Victims of cybercrimes often find themselves in a vulnerable position. The digital realm lacks the physical constraints of the real world, making it easier for criminals to perpetrate their actions with impunity. Protecting the rights and privacy of individuals in this digital age requires a delicate balance between upholding fundamental rights and ensuring security. For law enforcement agencies, it is a difficult terrain to navigate. Criminals can exploit the anonymity and pseudonymous nature of the internet to engage in illegal activities. This creates a criminal paradise of sorts, making it challenging to identify and apprehend wrongdoers.

In view of the above technological developments impacting the democratic society, the principles of the right to personal privacy and the right to life under Article 21, remain essential and more critical in the digital age. As we steer the complex landscape of the internet and data-driven technologies, it is crucial to find a harmonious balance that respects the individual's rights while safeguarding the collective security and integrity of the nation.

Privacy a Fundamental Right

To fully grasp the implications of privacy, one must delve into its multifaceted dimensions. First and foremost, personal privacy endows individuals with the power

to safeguard their personal information. This includes personal data such as one's medical records, financial transactions, correspondence, and digital footprints. In a world increasingly driven by technology, the ability to control and protect this data is indispensable. Privacy laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union, have emerged to secure individuals' rights in the digital age.

Additionally, privacy serves as a barricade against unwarranted surveillance. The right to be free from constant monitoring by governmental agencies or private corporations is essential to preserving democratic values. Excessive surveillance can have a chilling effect on free speech, inhibiting individuals from expressing dissenting opinions or engaging in activities that challenge the status quo. Hence, privacy ensures that individuals can voice their concerns and advocate for change without fear of reprisal. Furthermore, the right to personal privacy safeguards individuals from intrusive inquiries into their personal lives. This protection extends to the sanctity of one's home, personal correspondence, and family matters. It ensures that individuals can maintain their intimate relationships and personal secrets without undue interference.

Therefore, the personal privacy is not a mere luxury; it is the essential element of a just and equitable society. It allows individuals to flourish in an environment that respects their autonomy, dignity, and individuality. It is a right that transcends political, cultural, and geographical boundaries, as enshrined in the Universal Declaration of Human Rights. In a world marked by rapid technological advancements and increasing data-driven decision-making, the preservation of personal privacy becomes even more critical. It is incumbent upon democratic nations to safeguard this essential right and strike a delicate balance between security concerns and the protection of individual freedoms. In doing so, they uphold the very essence of democratic values and the dignity of every human being.

The inquiry into whether an individual's privacy constitutes a fundamental right is of profound significance, having engendered extensive legal and constitutional discourse. In the Indian context, this matter was unequivocally resolved by the Apex Court through the momentous Justice Puttaswamy Judgment in the year 2017. [2017) 10 SCC 1, AIR 2017 SC 4161]. Before the Puttaswamy Judgment, there was uncertainty regarding whether privacy was considered a fundamental right under the Indian Constitution. However, this ambiguity was put to rest when Justice Puttaswamy a petitioner challenged the use of Aadhaar, India's biometric identification system, on the grounds that it constituted an infringement of privacy. The Justice K.S. Puttaswamy and Others case, often referred to as the "Privacy as a Fundamental Right" case, was a landmark judgment delivered by the Supreme Court of India on August 24, 2017. The case revolved around the question of that Whether the right to privacy a fundamental right under Article 21 of the Indian Constitution. Here's a detailed analysis of this historic judgment:

Background: The case was triggered by a series of petitions challenging the ‘*Aadhaar program’*, a government initiative that sought to collect biometric and demographic

data of Indian citizens for various purposes, including the provision of government benefits. The petitioners argued that the program violated their fundamental right to privacy under Article 21 of the Constitution. The Indian government contended that privacy was not a fundamental right, or if it was, it could be limited by reasonable restrictions.

Significant features of the Judgment: The Justice K.S. Puttaswamy case stands as a watershed moment in the annals of Indian jurisprudence, resolutely cementing the right to privacy as an intrinsic fundamental right. In its epochal pronouncement, the Supreme Court unambiguously affirmed that privacy enjoys constitutional protection under Article 21, eloquently stating, "The Right to Privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution." The Significant features of the Judgment, in a nutshell, are as follows:

1. Privacy as a Fundamental Right: The Supreme Court, in this unanimous decision by a nine-judge bench, held that the right to privacy is indeed a fundamental right protected under Article 21 of the Constitution. The court declared that privacy is an intrinsic part of the right to life and personal liberty guaranteed by Article 21.
2. Overruling Previous Decisions: This judgment overruled two previous decisions by the Supreme Court that had suggested that privacy was not a fundamental right. The court explicitly stated that the judgments in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1962) no longer held valid with respect to the right to privacy.
3. Scope of the Right: The court recognized that the right to privacy is not an absolute right but is subject to reasonable restrictions in the interest of national security, public order, and other legitimate concerns. However, such restrictions must meet the tests of legality, necessity, and proportionality.
4. Informational Privacy: The judgment acknowledged various dimensions of privacy, including bodily integrity, personal autonomy, and informational privacy. It emphasized that the right to control one's personal information and data is a crucial aspect of privacy.
5. Balancing Individual and State Interests: The court recognized that in an increasingly digital and interconnected world, balancing individual privacy rights with legitimate state interests is a complex task. It emphasized the need for a robust data protection regime and the importance of informed consent in data collection.
6. Future Implications: The judgment had far-reaching implications, especially with regard to data protection laws and government surveillance programs. It laid the foundation for the drafting and implementation of the Personal Data Protection Bill, which aimed to regulate the processing of personal data in India.

This momentous decision underscored that every individual possesses the right to privacy as an indispensable facet of their right to life and personal liberty. Nonetheless,

it is imperative to recognize that this fundamental right to privacy remains subject to judicious restrictions imposed by law, indispensable for safeguarding the security and welfare of the state and its populace.

This landmark decision has left an indelible mark on the landscape of data protection, surveillance practices, and individual freedoms in the digital age. Its far-reaching implications can be succinctly encapsulated as follows:

1. Expanding Fundamental Rights: The ruling ushered in a profound expansion of fundamental rights in India, with the recognition of the right to privacy as an intrinsic component of the right to life and personal liberty. This pivotal stride represents a monumental leap in safeguarding individual liberties.
2. Data Protection and Regulation: The judgment's unequivocal emphasis on data protection and the significance of informed consent has laid the foundation for the development of comprehensive data protection legislation in India, exemplified by the emergence of the Personal Data Protection Bill.
3. Increased Accountability: It has catalysed heightened scrutiny of government surveillance programs, compelling a critical examination of the imperative need for surveillance reform. This recalibration aims to ensure that the sacrosanct boundaries of individual privacy rights remain inviolate.
4. International Recognition: On the global stage, this judgment has garnered international acclaim for its pivotal role in shaping the discourse surrounding privacy and data protection. Its resonance reverberates far beyond national borders, underscoring its influence on the broader global conversation.

In the digital age, privacy has taken on new dimensions, and cyberspace has become both a haven and a challenge for privacy rights. For example, in places like Jamtara, a region in the Indian state of Jharkhand, there are concerns about cybercafes being used for fraudulent activities, often referred to as the "phish pond." Cybercafes in Jhariatand, Karmatand, and Taratand have been notorious for facilitating cybercrimes such as phishing, identity theft, and financial fraud. According to this survey of Future Crime Research Foundation (FCRF), 80 % of Cyber Crimes in India happen through 10 districts such as Bharatpur, Mathura etc., named as “Dark Villages of India”. Globally, the prevalence of growing of cybercrimes on top gear is of greater concern. Financial crimes in cyberspace have doubled in some regions, including India, when compared to previous years. Reports indicate that these activities have spread across 81 countries, more than doubling their impact. Cybercrimes range from financial fraud to cyberterrorism and even cyber warfare. This rise in cybercrime poses significant challenges to law enforcement agencies. How can they combat the unregulated illegal flow of data across borders while simultaneously protecting the privacy and fundamental rights of individuals?

Balancing the need for security and the protection of fundamental rights, including privacy, in an increasingly interconnected and digital world is a complex task. It

requires constant vigilance, international cooperation, and the adaptation of legal frameworks to address the evolving nature of cybercrimes and cyber threats. Ultimately, the recognition of privacy as a fundamental right is a critical step in safeguarding individual liberties in the face of these challenges.

Privacy laws Around the World

Privacy laws are enacted to safeguard individuals' personal information from unauthorized access, use, or disclosure. Privacy laws around the globe are a complex and rapidly evolving field of legislation designed to protect individuals' personal information and data. These laws are rooted in the fundamental human right to privacy and have become increasingly important in our digital age, where vast amounts of personal information are collected, processed, and shared. These laws regulate how organizations and governments collect, store, process, and share personal data. Here are some significant privacy laws from different parts of the world:

European Union (EU) - The General Data Protection Regulation (GDPR) implemented in 2018, is one of the most comprehensive privacy laws globally. It applies to all EU member states and regulates the processing of personal data. GDPR grants individuals several rights, including the right to access their data, the right to be forgotten, and the right to data portability. It also imposes strict requirements on organizations handling personal data, including data breach notification and data protection impact assessments. It is one of the most influential privacy regulations globally. It grants individuals significant control over their personal data and imposes strict requirements on organizations, including data breach notifications and the appointment of Data Protection Officers (DPOs). GDPR also establishes hefty fines for non-compliance.

United States - The United States lacks a single, comprehensive federal privacy law. Instead, it has various state laws like the California Consumer Privacy Act (CCPA) and sectoral laws, such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data and the Gramm-Leach-Bliley Act (GLBA) for financial data. The privacy landscape in the U.S. is fragmented and evolving.

Canada - Personal Information Protection and Electronic Documents Act (PIPEDA) governs the collection, use, and disclosure of personal information by private sector organizations. It grants individuals rights to access their information and request corrections. It also mandates data breach notification.

Japan - Act on the Protection of Personal Information (APPI) regulates the handling of personal information by businesses. It includes principles like the necessity principle (collect data only for specific purposes) and the accuracy principle (maintain data accuracy).

Australia - The Privacy Act covers the handling of personal information by Australian government agencies and some private sector organizations. It includes the Australian Privacy Principles (APPs) that set out how personal information should be collected, used, and disclosed.

China - Personal Information Protection Law (PIPL): The PIPL, effective in November 2021, regulates the collection and processing of personal information in China. It includes provisions for consent, data localization, and cross-border data transfers.

The legal framework of protection of personal data generally consists of the following framework.
1. Consent: Individuals must give clear, informed, and voluntary consent for the collection and processing of their data. They should be able to withdraw consent at any time.
2. Purpose Limitation: Data should be collected for specified, legitimate purposes and not used for unrelated or excessive purposes.
3. Data Minimization: Only the minimum amount of data necessary for the intended purpose should be collected and processed.
4. Accuracy: Data must be accurate, and reasonable steps should be taken to keep it up to date.
5. Security: Organizations must implement appropriate security measures to protect personal data from breaches and unauthorized access.
6. Data Subject Rights: Individuals (subjects or principal) have rights to access, rectify, delete, or port their data, and they should be able to exercise these rights easily.
7. Accountability: Organizations are responsible for complying with privacy laws and must demonstrate compliance through policies, procedures, and records.
8. Cross-Border Data Transfers: Some laws restrict the transfer of personal data across borders, and organizations must ensure that adequate safeguards are in place for international data transfers.
9. Accountability and Transparency: Organizations should be transparent about their data practices, including data handling policies and data breach notifications. They should also appoint data protection officers and conduct privacy impact assessments. In the event of a data breach, organizations are often required to notify affected individuals and authorities within a specified timeframe.
10. Penal measures: Privacy laws typically include provisions for enforcement and penalties for non-compliance, which can include fines, sanctions, or legal actions. The entities who flout the legal procedures resulting in breach of personal data are subjected to penal measures. They are made to pay damages to the victims for the harms caused due to such breach.
11. Special Categories: Some laws provide extra protection for sensitive data categories, such as health information or biometric data

Privacy laws and principles of protection are critical for safeguarding individuals' personal information in an increasingly data-driven world. These laws and principles aim to strike a balance between individuals' privacy rights and organizations' need for data to provide services and make informed decisions. Staying compliant with these laws is not only a legal requirement but also essential for building trust with customers and stakeholders in today's digital age. Privacy laws and principles of protection continue to evolve in response to technological advancements and societal needs. Adhering to these laws and principles is not only a legal requirement but also crucial for building trust with individuals and protecting their fundamental right to privacy in our increasingly data-driven world.

Exploring Privacy Doctrines Worldwide

Privacy laws worldwide are designed to protect individuals' right to privacy in an era of increasing data collection and digitalization. These laws incorporate various legal doctrines and principles to address privacy concerns effectively. Some of the key doctrines in privacy laws around the world are as follows.

1. Consent: This is a central doctrine in privacy laws globally. It emphasizes an individual's right to control the collection, processing, and sharing of their personal data. Privacy laws typically require organizations to obtain clear and informed consent from individuals before processing their data. Consent ensures that individuals have a say in how their personal information is used. It safeguards against unauthorized data processing and provides individuals with the autonomy to make informed decisions about their data.

2. Purpose Limitation: This doctrine states that personal data can only be collected and processed for specific, legitimate purposes. Any deviation from these purposes may require additional consent or a lawful basis for processing. Purpose limitation prevents data from being exploited or used for unrelated purposes. It safeguards against "function creep" and ensures that organizations collect and use data only for the reasons individuals provided it.

3. Data Minimization: This is the practice of collecting only the minimum amount of personal data necessary for the intended purpose. It discourages the excessive collection of data. Data minimization addresses concerns about overreach and the potential for organizations to collect more information than is genuinely needed. It limits the risk of misuse and data breaches.

4. Data Subject Rights: These rights are fundamental to privacy laws. They grant individuals various rights, including the right to access, rectify, delete, or port their data. These rights empower individuals to control their personal information. Data subject (Principal as in India) rights enable individuals to exercise control over their data. They

are instrumental in holding organizations accountable for the accuracy, security, and lawful processing of personal data.

5. Data Security: Privacy laws often require organizations to implement robust data security measures to protect personal information from breaches and unauthorized access. Data security addresses concerns about data breaches, identity theft, and unauthorized access. It ensures that organizations take adequate measures to safeguard sensitive information.

6. Cross-Border Data Transfer: With global data flows, privacy laws address cross-border data transfers. They may require organizations to implement safeguards, such as standard contractual clauses or binding corporate rules, to protect data when it is transferred internationally. Cross-border data transfer rules address concerns about the privacy of data when it moves across jurisdictions with varying privacy standards. They protect data against potential risks associated with international transfers.

7. Accountability and Compliance: Privacy laws emphasize accountability, requiring organizations to demonstrate compliance with data protection regulations. This may involve appointing data protection officers, conducting privacy impact assessments, and maintaining records of data processing activities. Accountability ensures that organizations take privacy seriously and actively work to comply with the law. It addresses concerns about negligent or careless data handling.

8. Special Categories of Data: Privacy laws identify special categories of data, such as health or biometric data, and impose additional safeguards for their processing. These categories often have stricter requirements to protect sensitive information. Special categories of data are subject to additional protection due to their sensitive nature. This doctrine safeguards against potential discrimination or harm associated with the misuse of such data.

9. Data Breach Notification: Privacy laws may require organizations to promptly notify both authorities and affected individuals in the event of a data breach. This ensures transparency and enables individuals to take protective measures. Data breach notification addresses concerns about the secrecy of breaches and the potential harm to individuals. It enables swift action to mitigate the impact of breaches.
Conclusion:

Privacy laws around the globe incorporate a range of legal doctrines and principles to address various privacy concerns effectively. These doctrines, including consent, purpose limitation, data minimization, data subject rights, data security, cross-border data transfer rules, accountability, special categories of data, and data breach notification, collectively aim to protect individuals' privacy rights in an increasingly data-driven world. By adhering to these principles and doctrines, organizations and

governments can ensure responsible and respectful handling of personal data while upholding the fundamental right to privacy.

Protection of Personal data – Indian Legislative History

As of 2017, India did not have a standalone law on personal data protection. The legislative history of personal data protection in India has been a journey marked by the recognition of the importance of safeguarding individuals' digital privacy. Up until the DPDP Act of 2023 was passed, India lacked a dedicated law exclusively aimed at safeguarding personal data. However, personal data protection had found its place in the Information Technology (IT) Act of 2000, primarily under section 43A. Use of personal data was regulated under section 43A of the Information Technology (IT) Act, 2000 as amended read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. However in the DPDP Act of 2023 the above provision has been omitted vide subsection (2) of section 44 of the PDPD Act 2023.

"*Information Technology (IT) Act of 2000 - Section 43A : Compensation for failure to protect data.*--*Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation. --For the purposes of this section, --

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.] 1 Ins. by s. 22, ibid. (w.e.f. 27-10-2009)".

Section 43A of the Information Technology Act, 2000 (ITA), was the crucial provision that dealt with the liability of a body corporate for failing to protect sensitive personal data or information. This provision had significant implications for data protection and cybersecurity in India. A detailed analysis of Section 43A is as under:

1. Scope of the Section: Section 43A applied to "body corporates," which includes companies, firms, sole proprietorships, and associations of individuals engaged in commercial or professional activities. It was pertaining to situations where a body corporate possesses, deals with, or handles sensitive personal data or information in a computer resource that it owns, controls, or operates.

2. Liability for Negligence: The central element of Section 43A was that the body corporate can be held liable if it is found to be negligent in implementing and maintaining reasonable security practices and procedures.

3. Wrongful Loss or Gain: The negligence mentioned above must result in either wrongful loss or wrongful gain to any person. This implies that if a breach of data security causes financial harm to an individual or unjust enrichment to another, the body corporate is liable for compensation.

4. Compensation for Affected Parties: The primary consequence of a breach under Section 43A was the obligation of the body corporate to pay damages by way of compensation to the person(s) affected by the breach.

5. Reasonable Security Practices and Procedures: The section refers to "*reasonable security practices and procedures*." These are measures designed to protect sensitive personal data from unauthorized access, damage, use, modification, disclosure, or impairment. The ITA allowed for flexibility in defining these security practices and procedures. They may be specified in an agreement between the parties involved or in any law currently in force. In the absence of specific agreements or laws, the Central Government, in consultation with relevant professional bodies or associations, has the authority to prescribe what constitutes reasonable security practices and procedures. This section provided a degree of adaptability to evolving cybersecurity standards.

6. Definition of Sensitive Personal Data or Information: The section did not provide a detailed definition of "sensitive personal data or information." Instead, it empowers the Central Government, in consultation with relevant professional bodies or associations, to prescribe what constitutes such data. This allowed for flexibility in defining sensitive information to adapt to changing circumstances and technologies.

7. Significance: Section 43A is critical for data protection in India as it imposed a legal obligation on organizations to safeguard sensitive personal data. It acted as a deterrent against data breaches and encourages organizations to implement robust cybersecurity measures. It provided a legal avenue for individuals to seek compensation for damages resulting from data breaches.

8. Compliance and Enforcement: Compliance with Section 43A was essential for businesses and organizations that handle sensitive personal data. Non-compliance can lead to legal consequences, including the payment of compensation to affected individuals. The enforcement of this provision is essential to ensure the protection of individuals' privacy and data security.

Section 43A of the Information Technology Act, 2000, was a crucial legal provision in India that holds body corporates accountable for the protection of sensitive personal data. It emphasizes the importance of implementing reasonable security practices and procedures and provides individuals with a legal recourse in the event of data breaches. This section played a pivotal role in data protection and cybersecurity in India's evolving digital landscape. Regrettably, the DPDP Act of 2023 left out this provision, resulting in the nullification of remedies previously accessible to victims under Section 43A and the corresponding regulations within the Information Technology Act of 2000.

The realization of the need for comprehensive data protection legislation during the proceedings relating to Aadhar implementation in the Justice Putaswamy case led to the formation of the Justice B. N. Srikrishna commission in 2017. This commission was tasked with addressing the landscape of data protection within the country, considering the growing significance of personal data in the digital age.

As stated above, the Hon' Supreme Court of India made a historic decision in the justice Puttaswamy case. The court held that the right to privacy is an intrinsic component of the broader right to life as outlined in Article 21 of the Constitution of India. This landmark decision underscored the fundamental nature of privacy rights in the Indian legal context and set the stage for the development of robust data protection laws. The legislative history of personal data protection in India has seen a significant evolution, driven by the recognition of the importance of privacy rights in the digital age. The journey from the justice Puttaswamy case to the introduction of the Digital Personal Data Protection Bill of 2023 reflects India's commitment to establishing a robust framework for the protection of personal data and digital privacy.

The Srikrishna commission diligently worked on its mission and submitted its comprehensive report in July 2018. The commission drafted the Personal Data Protection Bill (referred to as PDP for brevity), which was formally presented as the PDPB 2019 in the Indian Parliament during December 2019. The primary objective of this bill was to establish a framework for the responsible management of personal data, ensuring privacy and data protection in India that conformed to international standards, particularly the European Union's General Data Protection Regulation (GDPR). Among its provisions for protecting individual privacy, the draft legislation sought to empower individuals with greater control over the collection and use of their personal data and provide them with the ability to seek damages for any harm resulting from data breaches by fiduciaries. The mentioned judgment played a crucial role in shaping the PDP Bill, which aimed to regulate the processing of personal data and strengthen the rights of individuals concerning their personal information.

The PDPB underwent scrutiny by the Joint Parliamentary Committee (JPC), which concluded its findings in December 2021. However, the legislative process hit a roadblock in August 2022 when the bill was withdrawn. To address the concerns and improve the bill, a Draft Bill was released for public feedback in November 2022. This

allowed various stakeholders, including citizens and experts, to provide their input and suggestions.

After considering the inputs from various stakeholders, the Digital Personal Data Protection Bill of 2023 was presented in Parliament on August 3, 2023. This bill represented a comprehensive effort to protect personal digital data in the country. Under the provisions of this bill, the processing of digital personal data would require the consent of the individual concerned, establishing consent as a principal regulation. Furthermore, personal data held by fiduciaries would be subject to stringent regulations to avoid breaches and protect individuals' privacy rights. The bill also proposed for the establishment of a Data Protection Authority with the authority to regulate and enforce data protection laws, ensuring that individuals' personal data is handled responsibly and securely. The DPDP Bill was enacted as the DPDP Act 2023 on August 8, 2023.

The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), (herein after referred to as ‘the Act’ for brevity) is a pivotal piece of legislation aimed at governing the processing of digital personal data. It embodies the dual recognition of the right of individuals to protect their personal data and the necessity to process such data for lawful purposes. The DPDPA, 2023, is a comprehensive piece of legislation that aims to strike a balance between the protection of individuals' personal data and the legitimate needs of organizations to process such data. It sets forth a structured legal framework for the collection, storage, and use of personal data, providing individuals with rights and remedies in case of data breaches or violations. The Act is structured into nine chapters, consisting of 44 sections, each addressing different aspects of digital personal data protection and regulation details of which are as follows:

CHAPTER I - Preliminary [Sections 1 to 3]: This chapter provides the foundational framework for the Act, defining key terms and concepts related to personal data protection and establishing the Act's objectives and scope.

CHAPTER II - Obligations of Data Fiduciary [Sections 4 to 10]: This chapter lays down the responsibilities and obligations of data fiduciaries, entities that collect and process personal data. It covers various aspects such as grounds for processing personal data, the requirement for providing notice to data principals (individuals), obtaining consent, and outlines certain legitimate uses of personal data. It also sets out the general obligations of data fiduciaries and additional obligations for significant data fiduciaries who deal with a large volume of data.

CHAPTER III - Rights and Duties of Data Principal [Sections 11 to 15]: This chapter focuses on the rights and duties of data principals, which are the individuals whose personal data is being processed. It outlines their right to access information about their personal data, request correction and erasure of data, seek grievance redressal, and nominate a representative for data protection matters. It also specifies the duties of data principals in ensuring accurate and lawful data processing.

CHAPTER IV - Special Provisions [Sections 16 and 17]: This chapter addresses specialized provisions related to the processing of personal data outside India and specifies exemptions under certain circumstances.

CHAPTER V - Data Protection Board of India [Sections 18 to 26]: This chapter establishes the Data Protection Board of India, which plays a crucial role in overseeing and regulating data protection in the country. It outlines the composition, functions, and powers of the board.

CHAPTER VI - Powers, Functions, and Procedure to be Followed by Board [Sections 27 and 28]: This chapter delves deeper into the powers and functions of the Data Protection Board and outlines the procedural aspects that the board must follow in its operations.

CHAPTER VII - Appeal and Alternate Dispute Resolution [Sections 29 to 32]: This chapter provides a mechanism for individuals and entities to appeal decisions made by the Data Protection Board. It also outlines the processes for alternate dispute resolution in data protection matters.

CHAPTER VIII - Penalties and Adjudication [Sections 33 and 34]: This chapter specifies penalties for non-compliance with the Act and the adjudication process for determining violations and imposing penalties.

CHAPTER IX - Miscellaneous [Sections 35 to 44]: This final chapter contains miscellaneous provisions, including provisions related to the central government's power to make rules, transitional provisions, and the Schedule.

The Digital Personal Data Protection Act, 2023, is a significant step forward in India's efforts to align with global data protection standards and protect the digital privacy of Its Citizens.

Key Features of The DPDP Act

The DPDP Act introduces a range of key features that are integral to its framework for safeguarding personal data in India. These features are designed to ensure that individuals have control over their personal data while allowing lawful data processing for legitimate purposes. Some of the key highlights that are pivotal to understanding its scope and implications are deliberated in brief in the following part.

1. Applicability: The Act applies to the processing of digital personal data within India, whether it is collected online or offline and subsequently digitized. It also extends its jurisdiction to the processing of personal data outside India if it is for offering goods or services to individuals in India. The term "processing" encompasses activities such as collection, storage, use, and sharing of personal data. This extra-territorial applicability ensures that entities operating abroad are also held accountable for protecting Indian citizens' data.
2. Lawful Purpose and Consent: Personal data may only be processed for a lawful purpose with the explicit consent of the individual. Prior to seeking consent, data

fiduciaries (entities processing the data) are required to provide a notice detailing the personal data to be collected and the purpose of processing. Importantly, individuals have the right to withdraw their consent at any point in time. However, consent is not required for "legitimate uses," including specified voluntary sharing of data, provision of government benefits or services, addressing medical emergencies, and employment. Personal data may only be processed for lawful purposes, and this processing must be based on the consent of the individual, referred to as the "Principal." Consent plays a central role in determining the legitimacy of data processing activities.

3. Specified Legitimate Uses: While consent is crucial, the Act recognizes certain legitimate uses of personal data that do not require explicit consent. These include instances where individuals voluntarily share their data and situations where the State processes data for permits, licenses, benefits, and services.

4. Data Fiduciary Obligations: Entities that collect and process personal data, known as data fiduciaries, are obligated to adhere to stringent rules. They must maintain the accuracy of data, ensure its security, and delete data once its purpose has been fulfilled. These obligations underscore the responsibility of organizations in safeguarding individuals' data.

5. Rights of Data Principals: The Act grants certain rights to individuals, referred to as data principals. The Rights include:

    - Right to access information about personal data
    - Right to correct, complete, update and erasure of the personal data provided
    - Right to nominate any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data.
    - Right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager.

    There are also duties mandated for the principal to follow, namely-

    - comply with the provisions of all applicable laws for the time being in force while exercising their rights under the provisions of this Act.
    - to ensure not to register a false or frivolous grievance or complaint.
    - to ensure not to suppress any material information while providing personal data for any document.
    - to ensure not to impersonate another person while providing personal data for a specified purpose.

    Data principals also have certain duties, such as not filing false or frivolous complaints, with violations punishable by penalties of up to Rs 10,000. These provisions empower individuals to have control over their personal data.

6. Exemptions for Government Agencies**:** The Central government has the authority to exempt government agencies from certain provisions of the Act under specified grounds. These grounds include concerns related to the security of the state, public order, and prevention of offenses. Specific exemptions are provided for certain cases, such as the prevention and investigation of offenses and the enforcement of legal rights or claims. This provision balances national security interests with data protection.

7. Data Protection Board of India: The Act establishes the Data Protection Board of India, a regulatory body with the power to adjudicate on non-compliance with the Act's provisions. This board plays a crucial role in enforcing and overseeing data protection laws in the country, ensuring that organizations adhere to their obligations.

   The Board is a body corporate with perpetual succession, a common seal, and powers to acquire, hold, dispose of property, contract, sue, and be sued. Key functions of the Board include- Monitoring compliances and imposing penalties, directing data fiduciaries to take necessary measures in the event of data breach, Hearing grievances made by affected persons. The Board has powers to Inspect documents of Companies handling personal data, Summon and examine individuals under oath, recommend blocking access to intermediaries that repeatedly breach the provisions. Appeal against the decisions of the Board will lie with TDSAT (Telecommunications Dispute Settlement and Appellate Tribunal)

8. The obligation of data fiduciary - A data fiduciary plays a vital role in the processing of personal data and the onus of protection of those data lies with him. A data fiduciary may process the personal data of an individual in accordance with the provisions of the Act and for a lawful purpose for which the consent is given or for certain legitimate use. While asking for consent from a data principal, a data fiduciary shall also give notice beforehand or at the moment of informing the purpose of data processing, rights of data principal and manner in which the data principal may make a complaint to the Board. Under Section 8(5) of the Act, A data Fiduciary is a duty bound to protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent a personal data breach.
9. Data breach and penalty - The Act states that in the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal intimation of such breach in such form and manner as prescribed. The lapses in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach may result in penalty of 250 crore rupees.

10. Significant step in protection of the digital privacy: The Digital Personal Data Protection Act, 2023, marks a significant step in India's efforts to protect the digital privacy of its citizens. It creates a legal framework that balances the need for

legitimate data processing with the protection of individuals' personal data. By establishing clear rules, obligations, and rights, the Act aims to enhance data security and privacy in an increasingly digitized world.

11. Transfer of Personal Data Outside India: The Act permits the transfer of personal data outside India unless restricted by the central government through notification.

In the upcoming parts of this series, we will provide an in-depth analysis of each of the provisions.

Mr. M. G. Kodandaram, IRS.
Assistant Director (Retd)
ADVOCATE and CONSULTANT