

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed Edition :

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

IJLRA

EDITORIAL TEAM

EDITORS

Megha Middha



Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain



Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8 Articles in various reputed Law Journals. Conducted 1 Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC - NET examination and has been awarded ICSSR - Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS
ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

SECURING THE DIGITAL LANDSCAPE: AN IN-DEPTH ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY- SEJAL RAGHUWANSHI
MAHARASHTRA NATIONAL LAW UNIVERSITY, NAGPUR

EMAIL: sejalraghuwanshi@nlunagpur.ac.in

CONTACT NO.: +91-8109739192

I. ABSTRACT

As our society gets more digitalized, effective legislations are more important than ever in order to protect personal data of individuals. This research paper explores the nuances of the Digital Personal Data Protection Act, 2023, a crucial piece of legislation designed to assist with the issues brought about by the constantly changing digital landscape. To begin with, the research paper explores whether the DPDP Act is a good law or not, i.e. whether it fulfills its purpose to protect the rights of individuals by protecting their personal data. To answer this, the research paper aims to provide an in-depth analysis of the DPDP Act, examining its key provisions, implications, and ongoing dynamics. The study evaluates the government's involvement in carrying out and upholding the Act and examining the duties and powers of the regulatory bodies. This paper, by carefully analyzing its language within the larger framework of digital privacy regulations, aims to highlight the consequences of the Act for individuals, businesses, and governmental agencies

that handle and process personal data. Further, the study draws a comparative analysis of the EUGDPR and the DPDP Act by drawing the similarities and differences between the two pieces of legislations, in order to discover areas of convergence, possible gaps, and best practices which would contribute to a worldwide understanding of efficient data protection methods. Eventually, this research contributes an in-depth understanding of the regulatory framework and its consequences for different stakeholders to the current discussions surrounding digital personal data protection. This research is a valuable resource for lawmakers, legal professionals, corporations, and individuals who are navigating the complex landscape of data protection and privacy in the twenty-first century, especially as the digital domain continues to grow.

Keywords: Data Protection, Digital, Personal Data, Privacy, Regulation, etc.

II. REVIEW OF LITERATURE

The KS Puttaswamy judgement, a significant legal milestone in India, marked a turning point in the recognition and strengthening of private rights within the framework of the constitution. Delivered on August 24, 2017, the Supreme Court upheld the right to privacy as a fundamental right guaranteed by the Indian Constitution. The dispute started as a result of concerns over the government's Aadhaar scheme. In addition to addressing the specific challenges associated with Aadhaar, the KS Puttaswamy ruling created a more comprehensive constitutional basis for the safeguarding of privacy as a fundamental component of individual liberty and human dignity. The verdict paved the way for a more nuanced understanding of privacy in the digital era, recognizing the dynamic obstacles presented by technological advancement and their influence on personal liberties. The KS Puttaswamy judgment has been the subject of significant study by academics and legal professionals who have explored its doctrinal significance, its role in reshaping the privacy legal landscape, and its potential influence on future legislative developments in the areas of individual rights and data protection. The KS Puttaswamy judgment is a cornerstone in Indian privacy law, and it continues to influence academic debate and the careful balancing act between individual rights and state interests.

III. INTRODUCTION

India's data protection policy achieved a major milestone with the enactment of the Digital Personal Data Protection (DPDP) Act 2023 on August 11, 2023.¹ The DPDP Act marks a significant step in translating the principles outlined in the 2017 Puttaswamy judgment into actionable implementation. The judgement held the right to privacy as a fundamental right under Art. 21 of the Constitution.² Since 2018, the legislature has been attempting hard to pass legislation, as seen by the formulation and scrutiny of several drafts, demonstrating a commitment to altering and adapting legal frameworks to meet changing societal requirements.

The legislation, which has been in the works for years, attempts to protect individuals' data while tackling the challenges of the digital age. The purpose of the Act is to govern the gathering, processing, and storage of digital personal data in a way that promotes innovation while upholding strict data protection requirements. In an endeavor to create a future where data is responsibly handled, India is dedicated to creating a safe and reliable digital environment for its individuals and companies which is evidenced by the DPDP Act.

The DPDP Act is a comprehensive legislative framework that promotes ethical and secure use of personal data, accountability, and transparency. The DPDP Act's principal objective is to ensure the ethical, responsible, and transparent use of personal data. It supersedes the earlier, more restrictive data protection laws with a comprehensive national framework for safeguarding personal data. Organizations that process personal data are subject to limitations and obligations under the act, which additionally provides rights for the individuals whose data is collected and used. These rights include obtaining individuals' consent before processing their personal data and establishing purpose limitation obligations. It is to be noted that the DPDP Act has not come into force yet. It will come into force through a notification issued by the Government of India in the Official Gazette.

¹ The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Gazette of India, August 11, 2023.

² Justice K.S. Puttaswamy and Anr. v. Union of India and Ors. (10 SCC 1, Supreme Court of India, 2017).

IV. KEY PROVISIONS

i. Scope and Application

The scope of the DPDP Act is notably extensive, encompassing a broad range of activities both domestically and abroad. The Act not only applies to citizens of India and Organisations that collect data of Indian residents, but it also includes non-citizens residing in India whose data is processed outside India “if such processing is in connection with any activity related to offering of goods or services”.³ It covers data which was originally offline or online, but later digitalized.

ii. Consent

The DPDP Act includes stringent provisions regarding consent for the processing of personal data. According to the Act, consent must be “free, specific, informed, unconditional, and unambiguous with a clear affirmative action.”⁴ This requirement is similar to the conditions set by the General Data Protection Regulation (GDPR), emphasizing the necessity for individuals to have the freedom to provide their consent.

The Act also deals with legacy data, for which companies may have previously received consent. Fiduciaries must provide these data principals the same notice as soon as “reasonably possible,” even though data processing might go on until the data principle to withdraw their consent.⁵ The Act prohibits the use of “bundled consent,” which means that there are stringent standards for purpose limitation. Furthermore, it gives data principals the freedom to withdraw their consent whenever they choose, just as simple as giving it in the first place.⁶ The DPDP Act states that Consent Managers accountable to data principals and act on their behalf. as per prescribed conditions.⁷ These provisions demonstrate the commitment that the Act is to guaranteeing that individuals are in complete control of their personal data and that they are informed before giving their consent for its processing.

³ The Digital Personal Data Protection Act, 2023, Section 3.

⁴ Ibid. Section 6.

⁵ Ibid Section 5(2)(b).

⁶ Ibid Section 6(4).

⁷ Ibid Section 6(8).

iii. Purpose of Data Collection

The Act allows the processing of personal data only for lawful means.⁸ Under the DPDP Act, the data fiduciary can process the data of an individual either through by the consent or for legitimate uses which has been defined in the act.⁹ Legitimate uses include where an individual has himself/herself voluntarily provided data for processing, sovereignty, security, fulfilling legal obligations, medical emergency, compliance with judgments, decrees, or orders, public disorders, etc.

iv. Rights of Users/ Consumers

The Act confers certain rights upon the data principals such as the right to obtain a summary of the data collected, the list of all other data processors and fiduciaries with whom the personal information has been shared, and a description of the data shared. Individuals also have the right to have their data revised, corrected, completed, and erased. They also have the right to nominate others who will receive personal data and to seek remedy for their issues.

v. Requirements for Data Localization

In regards to data localization, the Act stipulates that the government could limit flows to particular nations by notification.¹⁰ Although not stated clearly, it appears that the government's ability to impose restrictions on data transfers is derived from its legislative authority to safeguard national security. The law further specifies that this will not affect actions made by authorities that are sector-specific and may or may not impose localization requirements.

vi. Exemptions from obligations

The Act grants certain exemptions to the data fiduciaries from obtaining consent or complying with the notice requirements. Some of the exemptions include situations where processing is required to enforce a legal claim or right, when personal data has to be processed by courts or tribunals, when processing non-Indian residents' personal data within India or when processing is required for the prevention, detection, investigation, or prosecution of any offenses.¹¹

⁸ Ibid Section 4.

⁹ Ibid Section 7.

¹⁰ Ibid Section 16.

¹¹ Ibid Section 17(1).

V. ROLE OF GOVERNMENT AND OTHER AUTHORITIES

The DPDP Act empowers the government to play a significant role in its implementation. The government can seek information from data fiduciaries and designate particular entities as major data fiduciaries. However, the Act is being under criticized for granting the government arbitrary powers, possible ambiguities in interpretation, and for striking a delicate balance between promoting innovation and enhancing data protection.

The Act permits the government to set aside seeking consent when the beneficiary of government services has already been consented to receive any other state benefit.¹² As a result, the government may combine databases more easily by simplifying access to beneficiaries' personal information for government services. The Act exempts the government from several obligations, including notice and consent for processing for "prevention, detection, investigation or prosecution of any offense or contravention of any law".¹³ Although this makes sense, Section 17(2)(a) then grants the government power to notify any government agency a complete exemption from the act for the purpose of maintaining public order, sovereignty, security, integrity, and preventing incitement.

Furthermore, the government can declare that an enterprise will not be subject to any of the law's requirements within five years of the law's enactment.¹⁴ There is nothing specified as when this exception will be in effect, nor does it provide any instruction on how to apply this provision.

Likewise, the government possesses arbitrary authority to implement rules that exclude businesses from certain obligations for the processing of children's data. However, they require consent of the parents for the same. The government may exempt any business from the requirements mentioned under sec. 9(1) to 9(3) by prescribing certain conditions.¹⁵ Yet again, this clause is vague about the requirements that must be met, the basis for granting this exception, and other aspects. This clause can potentially be misappropriated as it fails to provide sufficient directions. This becomes problematic when one compares it to the principles of Indian administrative law,

¹² Ibid Section 7b.

¹³ Ibid Section 17(1)(c).

¹⁴ Ibid Section 17(5).

¹⁵ Ibid Section 9(4).

which state that legislation should not grant the implementing authorities excessive or unreasonable authority.¹⁶

The government is responsible for establishing the Data Protection Board (DPB), an independent agency tasked with enforcing the law. The government will set up rules regarding the appointment and selection of the board members. The board is an autonomous body, however with a restricted mandate. The board has a restricted mandate to supervise the prevention of data breaches, establish remedial measures, to undertake investigations, and to impose fines for violations with the law.¹⁷ The board is not a regulatory body and lacks the authority to establish rules or conduct codes or seek information in order to monitor operations of enterprises. It is limited to doing so while conducting inquiries. Overall, these discretionary powers pose the danger of undermining the objective of the Act, hence a deeper look at transparency and responsible use of power is required.

VI. IMPACT OF DPDP ACT ON INDIVIDUALS, BUSINESSES AND GOVERNMENT

i. Individuals

The DPDP Act seeks to give individuals greater authority over their data by giving them rights and imposing requirements on enterprises and other entities that gather, use, and retain personal data. Individuals can use these rights to restrict, access, correct, or remove their data. The Act's emphasis on user control reflects the growing global awareness of the importance of individual privacy in the digital era. Additionally, by striking a balance between technological progress and individual autonomy, the DPDP Act aims to promote trust among individuals and protect their data.

ii. Businesses

The new Act will have a significant impact since data is the basis of the consumer sector. The DPDP legislation pushes businesses to adopt modern privacy policies, employ technology that enhances privacy, and educate employees on how to handle personal information. D2C and online

¹⁶ A.N. Parasuraman etc. v. State of Tamil Nadu, SCC (4) 683; Agricultural Market Committee v. Shalimar Chemical Works Ltd. (1) SCR 164.

¹⁷ Ibid Section 27 and 28.

retailers must follow a variety of requirements, which means they must reconsider how they handle digital safety. Other parties in the ecosystem, such as merchants, call center companies third-party logistics, marketing companies, sales and distribution outsourcing firms, and payment facilitators, will also be included by the new Act.

The Act enables businesses to do gap analyses and implement remedial actions by promoting an awareness-based culture. The rule would force companies to alter how they collect, use, and keep personal data, which will add to their expenses and demands on resources. The framework for cross-border data transfer will help with compliance, draw in foreign investment, encourage new businesses, and enable the government to successfully manage data transfer issues.

iii. Government

Governmental organizations that handle and process personal data are similarly impacted by the DPDP Act. The statute grants the government the power to establish the Data Protection Board, an independent organization that can look into complaints from data principals. The board can impose legal sanctions on offenders and assign government agencies regulatory and enforcement responsibilities.

VII. EUGDPR AND DPDP ACT

Two important pieces of legislation, the Digital Personal Data Protection (DPDP) Act of India and the General Data Protection Regulation (GDPR) of the European Union, are designed to safeguard people's data privacy and provide them more control over their personal data. The GDPR, which came into force in 2018 is a comprehensive legislation that regulates the processing of personal data within the European Union (EU) and the European Economic Area (EEA). The DPDP Act is the first piece of law in India that gives people control over their data in order to safeguard it.

Although the GDPR and the DPDP Act use distinct regulatory methods, they both seek to preserve and protect data and privacy. The GDPR is a rule that applies consistently throughout the EU and EEA, whereas the DPDP Act is a principles-based law that is applicable universally to all types of digital personal data in India. Furthermore, the GDPR incorporates supplementary guidelines on the handling of sensitive personal data, including health records, political opinions, and religious

beliefs, which are not expressly covered by the DPDP Act.

One notable distinction among the two laws is that the DPDP Act applies uniformly to all types of digital personal data, but the GDPR places stricter limitations on the handling of sensitive personal data. Furthermore, in contrast to the GDPR, the DPDP Act grants the government the power to determine the dates on which certain Act sections would become operative. It also lacks the necessary transitioning phase.

Though it has distinct features and requirements that set it apart from the GDPR, the DPDP Act is inspired by the latter and has similar goals with regard to data protection and privacy.¹⁸ While each uses a different set of regulations, both laws seek to address the concerns brought up by the digital economy and the requirement to protect personal data.

VIII. CONCLUSION

The Digital Personal Data Protection (DPDP) Act is a comprehensive regulatory structure that promotes responsible use of personal data, accountability, and openness. But sometimes, certain clauses might be overly strict, jeopardizing individual right to privacy. With the enormous amount of discretionary power left in the hands of the central government, the effectiveness of the DPDP Act in protecting privacy will largely depend on the government's devotion to data security and privacy. The DPDP Act may lead to a highly centralized regulatory framework, posing privacy and data protection issues. Examples of these provisions are the extensive powers granted to the state and the exemption clauses for particular data fiduciaries. Notwithstanding these worries, the DPDP Act is a significant step towards improving data security and privacy in India as it offers people more control over their personal data and imposes obligations on the corporations that manage it.

¹⁸ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics & Information Technology, Government of India, July 27, 2018.