INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

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

 ISSN: 2582-6433

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 8Articles in various reputed Law Journals. Conducted 1Moot 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.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS 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.

ISSN: 2582-6433

DATA PRIVACY AS A FUNDAMENTAL RIGHT: ANALYSING INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - SNEHA CHAUHAN

Abstract

The advent of the digital age has transformed personal data into one of the most valuable assets of modern times, raising profound legal and ethical questions about data protection, individual autonomy, and state surveillance. Recognizing the pivotal role of data privacy in safeguarding constitutional liberties, India enacted the Digital Personal Data Protection Act, 2023 marking a significant milestone in the evolution of privacy jurisprudence post the Supreme Court's landmark Puttaswamy judgment (2017). This research paper critically analyses the legislative framework of the 2023 Act in light of India's recognition of privacy as a fundamental right under Article 21 of the Constitution.

The paper traces the historical evolution of privacy rights in India, examines the key provisions of the Act including consent architecture, data fiduciary obligations, cross-border data transfers, and regulatory mechanisms and evaluates its effectiveness in balancing individual rights with legitimate state interests.

Introduction

In an era where technological advancements and digital platforms permeate every aspect of human life, the protection of personal data has emerged as one of the foremost socio-legal concerns worldwide. The exponential rise in the collection, processing, and monetization of individual data by both state and private entities has prompted a global movement towards recognizing and safeguarding the right to privacy. For India the world's largest democracy and second-largest internet user base the enactment of a comprehensive data protection law had long been a constitutional imperative and legislative necessity.

The Digital Personal Data Protection Act, 2023 (DPDPA) is India's first standalone legislation aimed at regulating the processing of personal data. It seeks to give effect to the Supreme

 ISSN: 2582-6433

Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), wherein the Court unanimously affirmed that the right to privacy is intrinsic to the right to life and personal liberty under Article 21. The enactment of the DPDPA marks the culmination of nearly a decade-long deliberative process triggered by the 2017 judgment, spanning multiple expert committee reports, draft bills, and public consultations.

At its core, the Act purports to empower individuals termed as "Data Principals" by conferring them with enforceable rights over their personal data while simultaneously imposing obligations on entities processing such data, called "Data Fiduciaries." The legislation draws inspiration from international frameworks like the European Union's General Data Protection Regulation (GDPR) but is distinctly tailored to India's socio-economic and governance realities. However, the Act has not been immune to criticism. Civil society groups, constitutional experts, and industry stakeholders have raised concerns about sweeping exemptions granted to the government, the weakened independence of the proposed Data Protection Board, and potential compliance challenges for small and medium enterprises. Against this backdrop, this paper undertakes a comprehensive doctrinal and comparative analysis of the Digital Personal Data Protection Act, 2023.

The subsequent sections will:
Trace the evolution of privacy rights in India,
Critically examine the Act's salient provisions,
Compare India's data protection framework with global benchmarks,
Identify existing legal and policy challenges, and
Propose actionable recommendations for strengthening data privacy safeguards in India.

The Pre-Puttaswamy Era: Privacy as a Constitutional Value

The right to privacy in India, before its constitutional recognition, was not explicitly mentioned in the Constitution. The initial interpretation of the Indian Constitution under the Fundamental Rights was primarily centered on liberty and equality. However, as modern life and technology evolved, so did the need for privacy protection. In the early days of the Indian republic, the right to privacy was understood in a limited sense, largely related to personal space and property.

In **Kharak Singh v. State of Uttar Pradesh** (1963), the Supreme Court ruled that the

 ISSN: 2582-6433

Constitution did not explicitly recognize the right to privacy. The judgment held that the right to privacy was not absolute, and police surveillance did not violate fundamental rights unless it was unreasonable. The Court's judgment was seen as a restrictive interpretation, as privacy was merely implied within the framework of personal liberty under Article 21.

This restrictive understanding of privacy continued until the 1990s, when India witnessed the dawn of the Information Technology Revolution. With the introduction of the internet and information technology, individuals' personal data started to be processed, stored, and transmitted in digital formats, raising new privacy concerns. As such, the advent of technology began to challenge the earlier definitions of privacy.

Puttaswamy and the Recognition of Privacy as a Fundamental Right

The landmark moment in the evolution of privacy in India came with the Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) case. This case fundamentally changed the legal landscape by affirming that the right to privacy is indeed a fundamental right guaranteed under Article 21 of the Constitution of India.

The Puttaswamy judgment was a response to the growing concerns regarding government surveillance, the use of biometric data through the Aadhaar scheme, and the risks posed by the digitalization of personal information. In its ruling, the Supreme Court stated that privacy is intrinsic to the fundamental rights to life and personal liberty and is protected by the Constitution.

The Puttaswamy ruling also acknowledged that privacy is not an absolute right and must be balanced with other public interests such as national security and public order. However, it was clear that the government could not undermine the right to privacy without meeting strict constitutional standards, including necessity, proportionality, and judicial oversight.

This judgment was a milestone because it laid the groundwork for legislative reform in India regarding data privacy and protection. It led directly to the formation of the Justice Srikrishna Committee, which drafted the initial version of the Personal Data Protection Bill, 2018, which ultimately paved the way for the Digital Personal Data Protection Act, 2023.

 ISSN: 2582-6433

Overview of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) represents India's first comprehensive attempt to regulate data protection in the digital age. It is the culmination of years of deliberation, debate, and policy consultation, reflecting the country's commitment to safeguarding individual data privacy while fostering innovation and economic growth in the digital sector. The Act draws on the principles of the General Data Protection Regulation (GDPR) of the European Union, but is tailored to fit India's unique legal, economic, and technological context.

Key Objectives of the DPDPA

The primary objective of the DPDPA is to safeguard personal data of individuals (referred to as "Data Principals") from misuse, while ensuring that the use of such data remains within clearly defined legal and regulatory frameworks. The Act aims to establish transparency, accountability, and consent-based data collection as central tenets of the data processing ecosystem. The key objectives of the DPDPA include:

Protecting individual rights over personal data.

Establishing clear obligations for data fiduciaries (those who process data).

Strengthening enforcement mechanisms through an empowered Data Protection Authority (DPA).

Ensuring that personal data is processed fairly, lawfully, and transparently.

Definition of Personal Data

The DPDPA defines personal data as any information related to an identified or identifiable individual. This can include names, addresses, phone numbers, email addresses, biometric data, online identifiers, and other data that can be used to identify an individual. Furthermore, the Act categorizes personal data into two broad categories:

Sensitive Personal Data: Data that, if compromised, could cause significant harm to individuals. This includes financial data, health data, biometric data, sexual orientation, religious beliefs, etc.

Critical Personal Data: This category includes data that the government may designate as critical to national security and sovereignty. This data may be subject to more stringent regulations and localization requirements.

 ISSN: 2582-6433

Data Fiduciaries and Data Principals

The Act introduces the concept of Data Fiduciaries, who are the entities that determine the purpose and means of processing personal data. These fiduciaries can be public authorities, private companies, or any entity engaged in data processing. The Act imposes strict obligations on Data Fiduciaries, including the need to:

Obtain explicit consent from Data Principals for data collection.

Limit data processing to the purpose for which consent was given.

Take appropriate measures to safeguard the security and integrity of personal data.

Allow Data Principals to access and rectify their personal data.

Data Principals, on the other hand, are individuals whose data is being processed. The Act grants Data Principals several key rights, including:

Right to Access: Individuals have the right to obtain information about their personal data being processed.

Right to Erasure: Individuals can request the deletion of their personal data.

Right to Data Portability: Individuals can request that their data be transferred to another service provider.

Right to Consent: Consent must be informed, explicit, and revocable.

Cross-Border Data Transfers

One of the significant provisions of the DPDPA is its approach to cross-border data transfers. While the Act allows for such transfers, it imposes certain conditions to ensure that the data will be adequately protected in the recipient country. Data transfers can occur only to countries that have adequate levels of data protection in place, or if there are appropriate safeguards in place, such as binding corporate rules or standard contractual clauses.

In a controversial move, the Act also allows the Indian government to restrict cross-border data transfers of sensitive or critical data in certain circumstances, citing national security and public interest concerns.

Key Provisions and Their Analysis

Consent-Based Data Collection

One of the central pillars of the DPDPA is the concept of informed consent. Under the Act, personal data may only be processed if the Data Principal (individual) has given explicit,

 ISSN: 2582-6433

informed, and voluntary consent for its collection and use. This provision seeks to enhance transparency and accountability in data collection practices.

Analysis of the Consent Mechanism

The requirement for explicit consent is an important step toward ensuring that individuals have control over their personal data. However, it is important to evaluate the practicality and enforceability of this provision. The Act mandates that consent must be obtained in a clear and easily accessible manner, and individuals should be informed about the purpose of data collection, the scope of data being processed, and the duration of processing.

While the intention of this provision is to empower Data Principals, challenges arise in ensuring that consent is genuinely informed, especially in the case of complex or technical privacy policies. There is a growing concern about the "click-wrap" agreements used by tech companies, which often do not allow users to fully understand the implications of the data they are agreeing to share. The DPDPA requires that consent be freely given, but whether users are capable of understanding and meaningfully exercising this right is an area that requires close scrutiny.

Global Comparisons

In comparison to global standards, the GDPR of the European Union provides more detailed guidelines on obtaining consent, requiring that it be freely given, specific, informed, and unambiguous. Unlike GDPR, the DPDPA does not mandate a specific format for obtaining consent (e.g., checkboxes, opt-in procedures), which could lead to ambiguity in consent practices.

Data Localization Requirements

The DPDPA introduces data localization provisions that require certain categories of personal data to be stored within India. This is in line with similar provisions found in other countries such as Russia and China, which have also implemented stringent data localization policies.

Analysis of Data Localization

The Act categorizes personal data into three types: Personal Data, Sensitive Personal Data, and Critical Personal Data. While the first two categories can be transferred abroad, Critical Personal Data is required to be stored within India. The government is empowered to notify

 ISSN: 2582-6433

other categories of data that must be localized based on security and public policy concerns. Data localization is viewed as a contentious issue for various reasons. Proponents argue that storing data within the country ensures better control over data sovereignty and strengthens the enforcement of privacy rights. Additionally, it is seen as a measure to protect national security and prevent foreign surveillance.

On the other hand, critics argue that data localization may hinder cross-border data flows and impede the growth of the digital economy. Multinational companies may face higher compliance costs, and the overall efficiency of data processing could be reduced. Moreover, data localization could lead to fragmentation of the global internet, as data becomes siloed in various jurisdictions.

Global Comparisons

The GDPR does not require data localization, but it does regulate cross-border data transfers through strict adequacy requirements. Unlike the DPDPA, which allows the government to impose data localization measures, the GDPR allows for data transfers to non-EU countries based on the adequacy of the country's data protection laws.

The Data Protection Authority (DPA)

The Data Protection Authority (DPA) established under the DPDPA is tasked with overseeing the enforcement of the Act. The DPA has the power to investigate complaints, impose fines, issue penalties, and conduct audits of data processing entities.

Analysis of the Role and Powers of the DPA

The creation of an independent Data Protection Authority is a significant step toward ensuring the effectiveness of data protection laws. The DPA will be responsible for investigating breaches of data protection regulations, monitoring compliance, and providing guidance to businesses on how to comply with the Act’s provisions.

The DPA has a broad mandate to investigate complaints from Data Principals, issue fines for non-compliance, and take action against entities that violate the law. However, concerns exist regarding the independence and capacity of the DPA to effectively enforce data protection regulations, especially in the face of challenges posed by large multinational corporations. Additionally, the role of the DPA in interpreting the provisions of the Act may create some

 ISSN: 2582-6433

uncertainty, particularly in the absence of a clear framework for dispute resolution.

Global Comparisons

In comparison, the GDPR gives national Data Protection Authorities significant power, including the ability to impose heavy fines and sanction companies for non-compliance. These powers are designed to act as a deterrent against breaches of data privacy. The establishment of the DPA in India is a crucial step toward providing similar enforcement mechanisms.

Conclusion and Future Considerations

The Digital Personal Data Protection Act, 2023 is a significant milestone in India's journey toward protecting personal data and safeguarding privacy. It represents a shift in how personal information is collected, processed, and stored in the digital age. The Act's emphasis on informed consent, data localization, and strengthening enforcement mechanisms is crucial for building trust in the digital economy and protecting individuals' privacy rights.

However, the implementation of the Act will need to be closely monitored to ensure that its provisions are effective in practice. The challenge lies in balancing privacy protection with the demands of the digital economy, innovation, and international data flows. India's approach to data protection should evolve with technological advancements, ensuring that the rights of individuals are protected without stifling growth.

Further deliberations on data localization, cross-border data transfers, and ensuring the DPA's independence will shape the future of India's data protection regime. The DPDPA will likely undergo revisions and updates as the global landscape of data privacy continues to evolve, especially considering the rapid pace of technological change.

India's digital future will depend on how well the country integrates privacy, security, and innovation in its legal and regulatory framework. As more countries around the world look to India's example, it will be crucial for India to lead the way in shaping global standards for data privacy and protection.