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

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: DAWN OF DATA PRIVACY LAW IN INDIA

AUTHORED BY - ISHMEHAR KAUR SAHNI
LL.B. (Hons.), Amity Law School, Amity University, Uttar Pradesh

ABSTRACT

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a landmark legislative development in India's data governance landscape, enacted in partial fulfilment of the constitutional mandate flowing from the Supreme Court's recognition of the right to privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). This paper undertakes a detailed analytical study of the DPDP Act, examining its foundational principles, its salient features, the scheme of its nine chapters, and the definitional provisions governing data, personal data, and the right to data protection. It further analyses the territorial and extra-territorial scope of the Act under Section 3, the grounds of lawful processing, the rights and duties of data principals, the framework for cross-border data transfers under Section 16, exemptions under Section 17, and the institutional architecture of the Data Protection Board of India. The paper also addresses the Act's approach to the processing of personal data of minors and the additional obligations imposed upon Significant Data Fiduciaries. Drawing upon the Justice Srikrishna Committee Report, comparative judicial decisions including the CJEU's ruling in Google Spain v. AEPD, and allied legislative history, the paper argues that while the DPDP Act marks an important inaugural step in India's data protection journey, several lacunae including the absence of explicit provisions on automated decision-making, a limited right to object to processing, broad governmental exemptions, and the absence of a comprehensive cross-border transfer framework require further legislative attention if the Act is to be aligned with international standards of personal data governance.

Keywords: Digital Personal Data Protection Act 2023, data fiduciary, data principal, cross-border data transfer, consent, data sovereignty, fundamental right, India, DPDP Act, data governance.

ISSN: 2582-6433

INTRODUCTION

The Digital Personal Data Protection Act of 2023 represents a legislative attempt to reconcile the competing interests of individual data protection and lawful data processing, raising questions about the effectiveness of such a balance in the face of rapidly evolving digital landscapes and the increasing commodification of personal data.[1] The Act, is not the first piece of legislation designed to limit disclosure of information. The Indian law contains many instances of controls over specific aspects of privacy, covering, for example, law of Torts, trespass, negligence, nuisance, defamation, passing off, breach of confidence, law of contract or law of copyright. The Digital Personal Data Protection Act of 2023 marks a significant milestone in the protection of personal data, as it provides a broad and inclusive framework for data handling, grounding the right to digital data protection in Article 21 of the Constitution, thereby shielding citizens from the risks of informational privacy breaches emanating from both public and private entities. Data makes it possible to develop business models, gain an understanding of its customers, conduct effective marketing campaigns and develop its products and services. But just as for many other assets, there was a need for responsible use based on common rules. In light of the alarming rise in personal data breaches, which have exposed the sensitive information of millions, the Digital Data Protection Act of 2023 seeks to reassert individuals' control over their personal data, while also imposing stringent penalties on companies that fail to adhere to the regulatory framework, thereby underscoring the gravity of data protection. The relationship between privacy and information raises complex questions about the nature of personal autonomy and the role of governments in regulating the flow of information. While the notion of privacy is often predicated on the idea that individuals have a proprietary interest in their personal information, the reality is that governments and other entities often collect and use this information for a variety of purposes, highlighting the need for robust regulatory frameworks that protect individuals' rights and interests while also acknowledging the complexities of information sharing in modern society. The Act is limited to computer data (digital data) because the computer posed a unique threat to individual privacy through their ability to store, link and manipulate large amounts of data. Protection is also limited to living individuals, excluding the data protection claims of legal persons. The evolution of the Digital Personal Data Protection Act, 2023 was a gradual process that commenced with the Justice Srikrishna Committee's recommendations, which laid the

[1] Anirudh Burman, Understanding India's New Data Protection Law, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en Last visited at March 2026.

ISSN: 2582-6433

groundwork for the Personal Data Protection Bill, 2019. Following its introduction in Lok Sabha, the Bill underwent a series of revisions and consultations, including a Joint Parliamentary Committee review and a public consultation on a revised draft. The Government's decision to withdraw and revise the Bill in response to changing circumstances ultimately led to the passage of the Act in August 2023, marking a significant milestone in India's data protection landscape.

4.1. Principles of the DPDP Act

The DPDP Act, 2023 represents a significant legislative development, as it establishes a unified framework that applies to both public and private entities, outlining specific responsibilities for data fiduciaries and empowering individuals with distinct rights. The Act's core principles serve as the foundation for its regulatory approach, shaping the obligations and entitlements of various stakeholders. The core elements of the legislation are as follows:

i. Reciprocal relationship between two key entities: the data principal, who provides personal data, and the data fiduciary, who collects and processes this data. This symbiotic relationship highlights the interconnectedness of these stakeholders, emphasizing the need for mutual understanding and cooperation in the management of personal data.[2]

ii. It confers upon individuals a suite of rights that enable them to exercise agency over their personal data, including the rights to confirmation, correction, access, erasure, and portability, as well as the right to be forgotten, which collectively serve to safeguard their digital identity.[3]

iii. The Act sets forth a comprehensive framework for safeguarding individual privacy rights, with guiding principles that inform the compliance framework and a mechanism for redressing grievances. The establishment of a Data Protection Authority (Board), an Appellate Tribunal, and the appointment of Adjudicating Officers underscores the Act's commitment to effective implementation and enforcement of the regulatory framework.[4]

iv. The Act serves as a catalyst for promoting economic growth, innovation, and entrepreneurship, creating an enabling environment that fosters the development of new ideas and initiatives.

[2] Section 2(i) and Section 2(j), The Digital Personal Data Protection Act, 2023.
[3] Chapter III, The Digital Personal Data Protection Act, 2023.
[4] Chapter V, VII, VIII of the Digital Personal Data Protection Act, 2023.

ISSN: 2582-6433

4.2. Salient Features of the Act

The salient features of the DPDP Act, 2023 are:

i. To promote several key concepts that form the bedrock of robust data protection practices, including a consent framework, purpose limitation, storage limitation, and data minimization, which collectively ensure that personal data is handled in a responsible and transparent manner;

ii. Requirement that data fiduciaries collect data only for a specific purpose and with the data principal's consent underscores the importance of a purpose-driven approach to data collection, one that balances organizational interests with individual rights and interests.

iii. Concept of data privacy implies that individuals possess inherent rights to exercise control over their personal data, encompassing the following prerogatives like access to personal data, data rectification, data erasure, updating of data, data portability and data restriction.

iv. The regulatory architecture entails the establishment of a dedicated oversight body, formally designated as the Data Protection Board of India (hereinafter referred to as 'the Authority'). The organizational structure of this entity shall comprise of a Chairperson, serving as the titular head and a maximum of six whole-time Members, whose appointments shall be facilitated by the Central Government.

v. Mandate of the Data Protection Board is threefold, with a paramount focus on safeguarding data principal interests, mitigating personal data misuse, ensuring legislative compliance and fostering data protection awareness.

4.3. Scheme of the Act

The DPDP Act, 2023 contains nine chapters and one Schedule.

Chapter I consists of sections 1 to 3; section 1 providing title to the Act and date of commencement of its provisions; section 2 providing meaning to the expressions such as "data", "personal data", "digital personal data", "data fiduciary", "data principal", "data processor" and various other expressions used in the Act; section 3 laying scope of the Act.

Chapter II consists of sections 4 to 10. The Act strikes a balance between enabling data use for legitimate purposes and protecting individual rights. Section 4 establishes the principle of lawful processing, requiring consent or adherence to legitimate uses. Section 5 reinforces this balance by requiring data fiduciaries to be transparent with individuals, clearly stating the purpose for which their data will be used. Section 6 of the Act underscores the importance of

ISSN: 2582-6433

ethical and responsible data processing practices. It mandates that personal data be processed in a fair and reasonable manner, prioritizing the privacy of the data principal and ensuring that processing aligns with the purpose for which consent was obtained. Section 7 explains what legitimate uses of the personal data for which consent is as for example, for the performance by the State of any function or for fulfilling any obligation or for compliance with any judgment, under any law; for responding to any medical emergency or for medical treatment; for ensuring safety and providing assistance during any disaster or breakdown of public order; etc. Section 8 deals with general obligations of data fiduciary; Section 9 of the Act specifically addresses the processing of personal data of minors, while Section 10 imposes additional obligations on significant data fiduciaries. These provisions of section 9 and 10 aims to ensure that the processing of personal data is carried out in a manner that is respectful of the rights and interests of data principals, particularly in cases where they may be more vulnerable.

Chapter III of the Act, spanning sections 11 to 15, articulates the rights and duties of data principals. Notably, data principals are vested with the rights to: (i) access information about their personal data; (ii) rectify or erase their personal data; (iii) seek grievance redressal; and (iv) nominate a representative to exercise their rights in specified situations. These provisions enable data principals to exercise agency over their personal data and ensure that their rights are protected. The duties are: the duty to comply with the provisions of applicable laws, duty to ensure not to impersonate or suppress any material information or to register a false or frivolous grievance, and the duty to provide information as is true and correct.[5]

Chapter IV of the Act (Sections 16 and 17) clarifies the Act's jurisdictional reach and identifies specific exemptions. Section 16 governs the transfer of personal data outside India, while Section 17 outlines exemptions for processing related to legal proceedings, law enforcement, and national security, demonstrating the Act's flexibility in addressing diverse situations.

Chapter V (sections 18 to 26) deals with establishment of Data Protection Board of India, its composition, salaries and remuneration of its chairman and members, its proceedings, powers of Chairperson, etc.

Chapter VI (sections 27 and 28) deals with powers and functions of the Board and the procedure to be followed by it.

Chapter VII (sections 29 to 32:) deals with appeal to Appellate Tribunal and alternate dispute resolution mechanism.

Chapter VIII (sections 33 and 34) deals with penalties and adjudication.

[5] Section 2(n), The Digital Personal Data Protection Act, 2023.

ISSN: 2582-6433

Chapter IX (sections 35-44) addresses miscellaneous provisions, including safeguards for actions taken in good faith, limitations on the jurisdiction of civil courts, and empowers the Central Government to issue directives, formulate rules, and resolve implementation challenges. The accompanying Schedule details the penalty amounts for violations of the Act and its associated rules.

4.4. Data, Personal Data and Data Protection Right

The Digital Personal Data Protection Act, 2023 (DPDP Act) aims to safeguard "digital personal data," which, as per Section 2(n) of the Act, refers to personal data in a digital format.

The Act defines "personal data" in Section 2(t) as any data that can be used to identify an individual. Additionally, "data" is defined in Section 2(h) as a representation of information, facts, concepts, opinions, or instructions that can be communicated, interpreted, or processed by humans or automated systems. The Act is limited to "digital personal data", i.e., personal data in digital form or in other words, "computer data". It is because computerised information system posed a unique threat to individual privacy as it enables storing, linking and manipulating large amount of data.

In *R v Brown*,[6] Lord Hoffman observed, "Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other People that certain things are none of their business is under technological threat." Computers posed a unique threat to individual privacy through their ability to store, link and manipulate large amounts of data.

Before the enactment of the DPDP Act, 2023, there was a presumption that data flows are an unadulterated good. This is only partially accurate. In Justice Srikrishna Report, it is stated "It is clear that several data flows can cause considerable harm. But more significantly, the treatment of free data flows as an intrinsic good, as the recent expose of data sharing practices by Facebook demonstrates, has placed the interests of the individual in whose name the information flows, as secondary to the interests of companies of various kinds which deal with the data."[7]

Data is representation of information. Data and information seem interchangeable. But it is not so. There is a distinction between the two. Data can be compared to raw inputs, while

[6] R v. Brown, 1996, All ER 545, 556.

[7] A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, Available at https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy Last visited on March 2026.

ISSN: 2582-6433

information represents the output. The intermediary step, known as processing, includes tasks like data manipulation (sorting, merging, tabulating) and computation, which often involves both archived and incoming data. In a ground-breaking ruling, the Court of Justice of the European Union (CJEU) declared that internet search engines like Google are responsible for how they handle personal data that appears on third-party websites. The decision, handed down on May 13, 2014, in the case of Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD), marked a major shift in the way we think about online data protection. Suddenly, search engines were on the hook for ensuring that personal data was processed in a way that respected individuals' rights.

"The activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as "processing of personal data" within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing."[8]

4.5. Scope of The Act

4.5.1. Introduction

Section 3 of the Digital Personal Data Protection Act, 2023 deals with the scope of the Act. The Act was enacted, as its preamble reads, to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. The purpose of the enactment is to protect digital personal data and to ensure that the processing of such data is done for lawful purposes.[9] Justice Srikrishna Report on Personal Data Protection had observed, "In a legislation for India, questions of scope and applicability must be answered according to our policy objective of securing a free and fair digital economy. This objective will be severely compromised if data of Indians is processed, whether in India or elsewhere, without complying with our substantive obligations. Implicit in this is the ability of the state to hold parties accountable, irrespective of where data might have been transferred, and particularly to be able to enforce such obligations against errant parties. At the same time this objective cannot be enforced in derogation of established rules of

[8] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) dated 13th May, 2014 ECLI:EU:C:2014:317.
[9] Section 3, The Digital Personal Data Protection Act, 2023.

ISSN: 2582-6433

international comity, respecting the sovereignty of other jurisdictions in enforcing its own rules." The law has jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected or otherwise processed in India. However, in respect of processing by fiduciaries that are not present in India, the law shall apply to those carrying on business in India or other activities such as profiling which could cause privacy harms to data principals in India. Additionally, personal data collected used, shared, disclosed or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is actually processed in India. However, the data protection law may empower the Central Government to exempt such companies which only process the personal data of foreign nationals do not present in India.

4.5.2. Ingredients of Section 3

Section 3 of the Digital Personal Data Protection Act, 2023 (DPDA provides that the Act shall apply to the processing of digital personal data:[10]

(a) within the territory of India where the personal data is collected – (i) in digital form; or (ii) in non-digital form and digitised subsequently.

(b) outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.

But it shall not apply to: - (a) personal data processed by an individual for any personal or domestic purpose; and (b) personal data that is made or caused to be made publicly available by – (i) the Data Principal to whom such personal data relates, (ii) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly.

Illustration: X, an individual, while blogging her views, has publicly made available her personal data on social media. In such case, the provisions of this Act shall not apply.

4.6. Processing Within and Outside India

The Act applies to processing of digital personal data within the territory of India and also outside the territory of India; in case of former, the activity of collecting personal data in digital form is within India and in case of the latter, the activity of processing is in connection with offering of goods or services to data principal within the territory of India. Thus, the Act applies to the processing of personal data of data principal who are within India or where processor is

[10] Section 3, The Digital Personal Data Protection Act, 2023.

ISSN: 2582-6433

outside India, but the processing activities are related to offering of goods or services to data principal within India.

The collection methods usually used by companies are surveys, observations, questionnaires, interviews, focus groups, online tracking, transactional data tracking, online marketing analytics, social media monitoring, form fills and registration data.

Justice Srikrishna Committee, observed: i. All personal data of persons present in India that is processed must be protected. This can be ensured by exercising jurisdiction over personal data which is processed in India. If personal data is collected, disclosed, shared or otherwise processed in India, the law will apply to the processing of such personal data irrespective of the following facts: where the fiduciary is incorporated, where the processing or any subsequent processing takes place. This is based on the principle of territoriality [Part of the cause of action in respect of transactions over the internet may occur in India even if there is no server in India involved and passive personality. ii. Personal data processed by Indian companies must be protected, irrespective of where it is actually processed. This is based on the principle of nationality as the company is located/incorporated within one's jurisdiction.

iii. Personal data processed in India by foreign entities must be protected. Similar to the ground above, any processing in India is within the scope of Indian law on the basis of territoriality, irrespective of the nationality of the entity processing it."

While criteria (ii) and (iii) are direct in their application, criterion (i) represents an instance of extended jurisdictional reach.

The DPDP Act 2023 establishes territorial jurisdiction over the processing of personal data in the following cases: (1) where personal data is collected, used, shared, disclosed, or otherwise processed within India. (2) however, to avoid overbroad jurisdiction, the law carves out an exception for personal data collected by non-Indian fiduciaries from individuals present in India, unless they are engaged in targeted or systematic activities; and (3) where Indian companies process personal data, regardless of the location of processing, although the Central Government may exempt processors that exclusively handle the personal data of non-Indian nationals not resident in India.

4.7. Non-Applicability of the Act

The DPDP Act excludes from its scope the processing of personal data that occurs extraterritorially, i.e., outside the territory of India. Moreover, as specified in clause (c) of section 3 of the DPDP Act, the law also carves out exceptions for personal data processed by individuals for personal or domestic purposes, as well as data that has been made publicly

ISSN: 2582-6433

available by the data principal or by any other person under a legal obligation to do so.

India's new data protection law has some important exceptions. For one, it doesn't apply to personal data that's used for purely personal or household reasons. Think of it like this: if you're keeping a personal address book or sharing family photos, you don't have to worry about the law. But that's not all - the law also makes exceptions for authorities who need to make personal data public for reasons like preventing or investigating crimes, or to protect national security or someone's individual rights. It's all about striking a balance between protecting personal data and keeping the public safe.

They are however, as per constitutional requirement, subject to the principles of proportionality, legality, and necessity. Historical and scientific research are additional exceptions to the right to privacy which may not be subjected to the principles of proportionality, legality, and necessity.

REFERENCES

A. Legislation

1. The Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
2. The Information Technology Act, 2000, No. 21 of 2000 (India).
3. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).
4. The Personal Data Protection Bill, 2019 (India) (withdrawn August 2022).

A. Cases

5. Justice K.S. Puttaswamy (Retd.) v. Union of India, AIR 2017 SC 4161; (2017) 10 SCC 1.
6. Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317 (CJEU, 13 May 2014).
7. R v. Brown [1996] 1 All ER 545.
8. Kharak Singh v. State of Uttar Pradesh, 1964 (1) SCR 332.
9. Mr. X v. Hospital Z, AIR 1999 SC 495.
10. District Registrar v. Canara Bank (2005) 1 SCC 496.

B. Reports and Committee Documents

11. Ministry of Electronics and Information Technology, Government of India, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians': Report of the

ISSN: 2582-6433

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018), available at https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy.

12. Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, Report of the Joint Committee on the Personal Data Protection Bill, 2019 (December 2021).
13. Anirudh Burman, Understanding India's New Data Protection Law, Carnegie Endowment for International Peace (2023), available at https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en.

C. Books

14. R. Kitchin, The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences (SAGE Publications, London, 2014).
15. L.A. Bygrave, Data Privacy Law (Oxford University Press, Oxford, 2014).

D. Journal Articles

16. G. Greenleaf, 'Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey' (2018) 147 Privacy Laws & Business International Report 10.
17. A. Chandrasekharan, 'The Digital Personal Data Protection Act, 2023: A Step Towards Privacy Protection in India' (2023) 19(2) Indian Journal of Law and Technology 45.