

ABHIDHVAJ LAW JOURNAL

[www.abhidhvajlawjournal.com]

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Editor In chief – Assistant Professor Mr. Janmejay Singh

Publisher & Founder – Vaibhav Sangam Mishra

Frequency – Quarterly (4 Issue Per year)

ISSN: 2583-6323 (Online)

Copyright © 2025 - 26

SEAMLESS DATA FLOW: AN ANALYSIS OF PRIVACY CONCERNS AND NEED FOR DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT,2023 IN INDIA

AUTHOR'S NAME – Manju M Mamachan, LL.B, Second Year.

INSTITUTION NAME – KLE Law College, Bengaluru.

Received on 7 February 2025, Accepted on 9 February 2025, Published on 14 February 2025

ABSTRACT:

With the rapid growth in the digital economy, the flow of data across borders has become an integral part of global connectivity and economic growth. India is on track to achieve an estimated digital GDP of $1 trillion by 2025, demonstrating its rapid rise as a digital leader. The Digital India program, which was launched in 2015 has revolutionized the country's digital infrastructure. The flow of data has become so volatile that it raises concerns about privacy, security, and misuse as businesses and consumers alike look to take advantage of digitalization. This necessitates the adoption of a rigorous standard of review by referencing ideas of human dignity and democracy embedded within the conception of constitutional morality. This growing reliance on digital platforms necessitated a robust framework for data protection in India. The rapid growth in technology has emerged the need for a regulatory framework, leaving individuals vulnerable to data misuse and breaches of privacy. The Digital Personal Data Protection Act 2023, proposed by India's Ministry of Electronics and Information, aims to allow the easy transfer of data across borders[1] and establish a regulatory body to oversee compliance and impose penalties for such misuse of personal data. The Digital Data Protection Act, of 2023, aims to address these concerns by balancing individual privacy with the need for data processing. The DPDP Act, of 2023 marks a crucial step toward protecting digital personal data in India. It establishes the legal principles and procedures for data collection, processing, and storage while acknowledging the importance of consent and accountability by entities handling data. However, questions remain about the sufficiency of this legislative framework in addressing the real challenges across the world posed by the easy flow of data AI protection of personal data[2]. This research paper aims to study India's unique socioeconomic condition, including its digital economy's rapid growth, analysis of the Digital Data Protection Act, 2023, and challenges of safeguarding personal data in this context.

[1] Ministry of Electronics, https://pib.gov.in/PressReleasePage.aspx?PRID=2090048 (last visited Jan. 20, 2025).
[2] GDPR, https://gdpr.eu/eu-gdpr-personal-data/ (last visited Jan. 20, 2025).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Keywords: Digital economy, Cross-border data flow, Data privacy, Data security, Data misuse, Data protection, Digital Personal Data Protection (DPDP) Act, 2023, Data collection, Personal data.

CHAPTER 01: INTRODUCTION:

1.1 Context and Significance of Data in the Digital Age

Today, Digitalization has brought a massive change across the world. The number of users engaged in the internet and technology has increased tremendously as it is the most reliable and easy source for connectivity across the world. While the information of every individual is circulated everywhere through internet networks, the chance of misusing such information is also very high. The impact of the digital age results in information on the internet being permanent. Humans forget, but the internet does not forget and does not let humans forget[3]. Any endeavour to remove information from the internet does not result in its absolute obliteration. The footprints remain[4]. It is, thus, said that in the digital world, preservation is the norm and forgetting a struggle.[5]

The need to regulate the use of personal information is necessary. The users should be regulated so that their privacy can be maintained. Through many cases, the judiciary has tried to pinpoint the need to formulate a legal framework for data protection. It is noted in the landmark case of K. S. Puttuswamy vs. UOI, 2017 in para 637 that how the state is in need of establishing a legal framework for the protection of an individual's personal information used without their permission. The text of the judgment is as follows: "I agree with Dr. D.Y. Chandrachud, J., that formulation of data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of privacy concerns and legitimate State interests[6], including public benefit arising from scientific and historical research based on data collected and processed. The European Union Regulation of 2016 of the European Parliament and of the Council of 27-4-2016 on the protection of natural persons with regard to the processing[7] of personal data and the free movement of such data

[3] India kanoon, https://indiankanoon.org/doc/189278808/ (last visited Jan. 20, 2025).
[4] Gopal Krishna, Right to Privacy and the Bhagavad Gita, Rediff (Jan. 20, 2025, 8:00 P.M.), https://www.rediff.com/news/column/right-to-privacy-and-the-bhagavad-gita/20170928.htm.
[5] K.S Puttuswamy vs UOI 2017 10 SCC 1
[6] Law matics, https://thelawmatics.in/the-regime-of-data-protection-supreme-courts-views/ (last visited Jan. 20, 2025).
[7] Legislation gov, https://www.legislation.gov.uk/eur/2016/679/introduction (last visited Jan. 20, 2025).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

may provide useful guidance in this regard[8]. The State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed. Thus, for e.g., if the posting on social media websites is meant only for a certain audience, which is possible as per tools available, then it cannot be said that all and sundry in public have a right to somehow access that information and make use of it."[9] In a similar case, para 328 also shows how the Union Government is responsible for ensuring the security of individuals' personal data: Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the State but from non-state actors as well[10]. We commend the Union Government on the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the State. The legitimate aims of the State would include, for instance, protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits.[11] These are matters of policy to be considered by the Union Government while designing a carefully structured regime for the protection of the data. Since the Union Government has informed the Court that it has constituted a Committee chaired by Hon'ble Shri Justice B.N.[12] Srikrishna, former Judge of this Court, for that purpose, the matter shall be dealt with appropriately by the Union Government, having due regard to what has been set out in this judgment.[13]

1.2 Objectives of the Study:

The research paper aims at identifying the following objectives:

1. To analyze the concept of seamless data flow in this digital era.
2. To identify the privacy concerns associated with the exchange of personal data in this digital ecosystem.

[8] Eur lex, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/pdf (last visited Jan. 20, 2025).
[9] K. S. Puttuswamy vs. UOI (2017) 10 SCC 1
[10] Counter currents, https://countercurrents.org/2017/08/right-to-privacy-judgement-highlights-and-full-judgement/ (last visited Jan. 20, 2025).
[11] Nasscom Community, https://community.nasscom.in/communities/government-schemes/aadhaar-authentication-good-governance (last visited Jan. 20, 2025).
[12] Live law, https://www.livelaw.in/supreme-court-said-right-privacy-judgment-read-judgment/ (last visited Jan. 20, 2025).
[13] K. S. Puttuswamy vs. UOI (2017) 10 SCC 1

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

3. To evaluate the rules and regulations subject to the data protection laws in India.[14]
4. To understand or recommend the need for strict and stringent laws for personal data protection.

1.3 Scope of the Research:

The study focuses on the concerns of misuse of personal data of an individual and the laws prevalent in India to regulate such exchange of data. Its emphasis is on the privacy issues raised by the unregulated use of personal data. It studies the regulatory framework established by the implementation of the Digital Personal Data Protection Act of 2023

1.4 Research Methodology:

1. A detailed examination of existing literature on the flow of data and data protection.
2. Study of Academic Reports and Research Papers of scholars and academicians.
3. The analysis of the legal framework related to Data Protection.
4. It also referred to various newspaper articles or editorial articles.

1.5 Literature Review:

1.5.1 The literature titled "The Digital Personal Data Protection Act, 2023: Recommendations for Inclusion in the Digital India Act"[15] Enumerates the attempt made by the government to establish a regulatory framework for data protection by bringing up India's" first data protection act, which is the DDPD Act, 2023. It discusses some of the implementation mechanisms adopted by the act. While the research paper addresses the provisions of the DPDP Act of 2023, a key gap remains in addressing privacy concerns, because of which the need for implementation of such a regulatory framework arises.

[14] Free Laws, https://www.freelaw.in/legalarticles/Data-Protection-Laws-in-India-Current-Scenario-and-Future-Prospects- (last visited Jan. 20, 2025).

[15] Ajaykumar S., Basrur A., & Sharma V. (2023). The Digital Personal Data Protection Act 2023: Recommendations for inclusion in the Digital India Act. ORF Online (Jan. 20, 2025, 8:00 P.M.) https://www.orfonline.org/wp-content/uploads/2023/10/ORF_SpecialReport_DigitalPersonalDataProtectionAct2023.pdf.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

1.5.2 The research paper titled "Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India"[16] Examines the effects of the DPDP Act[17] on digital nagriks in six sections, beginning with an explanation of the need for privacy laws. Evaluating the Act's effects on cross-border data flow, business implementation difficulties, and its capacity to keep up with quickly changing digital technologies represent the main research gaps. A robust digital economy depends on resolving these concerns in order to preserve a balance between privacy, smooth data flow, and technological developments. While the research paper addresses the provisions of the DPDP Act, 2023, a key gap remains in addressing the privacy concerns, because of which the need for implementation of such a regulatory framework arises.

1.5.3 The literature titled "Comments on the (Draft) Personal Data Protection Bill, 2018"[18] Comments on the 2018 Personal Data Protection Bill draft, which was created[19] by a committee of experts led by Justice B.N. Srikrishna, are included in this publication. We observe that, especially with regard to processing by commercial entities, the draft Bill provides a reasonably comprehensive set of data protection principles and rights to data subjects. While the research paper addresses the provisions of the DPDP Act, 2023, a key gap remains in addressing the privacy concerns, because of which the need for implementation of such a regulatory framework arises.

CHAPTER 02: UNDERSTANDING SEAMLESS DATA FLOW:

2.1 Humans on Continuous Surveillance

Is my smartphone listening to me? There is always an ongoing question going into one's mind. Popular virtual assistant apps like Siri give answers instantly with the use of a microphone. If you, as a consumer, give permission to use the microphone, it is very important to understand how personal information can be protected online through lots of

[16] Charru Malhotra, Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India, 70 Indian Journal of Public Administration (Jan. 20, 2025, 8:10 P.M.), https://journals.sagepub.com/doi/10.1177/00195561241271575?icid=int.sj-full-text.similar-articles.5.

[17] Abhishek Singh and Anusha, The Digital Personal Data Protection Act, 2023: An Ambitious Government Step Towards Ensuring Its Wide Reach, Sage Journal (Jan. 20, 2025, 8:10 P.M.), https://journals.sagepub.com/doi/abs/10.1177/00195561241271533?journalCode=ipaa.

[18] Bailey R., Bhandari V., Parsheera S., & Rahman F. (2018). Comments on the (draft) Personal Data Protection Bill 2018. National Institute of Public Finance & Policy (Jan. 20 2025, 8:15 P.M.), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269735

[19] Rishab Bailey, Vrinda Bhandari, Comments on the Draft of Personal Data Protection Bill 2018, Papers ssrn (Jan. 20 2025, 8:20 P.M.), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269735.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

mobile security available in the phone itself. It is very important to get answers to these questions, such as: Is my phone listening to me? What application or network it is listening to me? How is this information listened to by them? How it can be protected? Sometimes, you often observe that you see advertisements on the phone that you have recently talked about. Usually, misuse of the information from the phone happens because we have given consent to it consciously or unconsciously. Often, when we accept certain terms and conditions without reading them, such consent is automatically given, and that's how usually the flow of information from our mouth to our phone reaches. That's why it is very important to read the terms and conditions once so that we can know what information has been sent by phone. It is always wise to review the terms and conditions once and then give consent. Nowadays, even social media algorithms are trying to understand the behavioral patterns and likings of individuals, which results in tracking each and every data of a person. In one of the judgments of the Supreme Court, it was pointed out that "The right to privacy is directly infringed when there is surveillance or spying done on an individual, either by the State or by any external agency."[20] Ellen Alderman and Caroline Kennedy, in "Right to Privacy," foresaw this threat to privacy in 1995 while referring to governmental eavesdropping in the United States of America in the following words:

"Perhaps the scariest threat to privacy comes in the area known as "informational privacy." Information about all of us is now collected not only by the old standards, the IRS and FBI, but also by the MTB, MIB, NCOA, and NCIC, as well as credit bureaus[21], credit unions, and credit card companies. We now have cellular phones, which are different from cordless phones, which are different from what we used to think of as phones. We worry about e-mail, voice mail, and junk mail. And something with the perky name Clipper Chip developed specifically to allow governmental eavesdropping on coded electronic communications is - apparently the biggest threat of all."[22]

2.3 Privacy tips for smartphones:

[20] Manoharlal Sharma vs. UOI and others (2024) 11 SCC 401

[21] Advocate, https://www.advocatekhoj.com/library/judgments/index.php?go=2021/october/62.php (last visited Jan. 20, 2025).

[22] Case mine, https://www.casemine.com/search/in/electronic%2Bcommunications%2Bprivacy%2Bact%2Becpa (last visited Jan. 20, 2025).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

1. Download apps from the official website and avoid downloading them from third-party applications.
2. While giving consent to any terms and conditions, it should be properly read by the individual so that you can access up to what limit your information has been used by that particular app.
3. Avoid sharing unnecessary information if you don't feel it is necessary.
4. Always see the settings of the particular app downloaded by you so that you can make changes according to your use, like disabling, the microphone, disabling, the camera, et cetera. In this way, you can limit the power of the app to use your information.

CHAPTER 03: PRIVACY CONCERNS IN THE DIGITAL ECOSYSTEM:

3.1 What is Privacy?

American law professor Alan Westin defined privacy as "the claim of an individual to determine what information about himself or herself should be known to others."[23] According to Israeli law professor Ruth Gavison, "Our interest in privacy […] is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention."[24] American jurist and economist Richard Posner avoids giving a definition but states "that one aspect of privacy is the withholding or concealment of information."[25] American professor Charles Fried stated that privacy […] is the control we have over information about ourselves."[26]

In my opinion, privacy can be defined as that aspect of life that cannot be interfered with without permission or without any proper, lawful purpose. The personal information of the individual should not be misused. Privacy is an individual's basic right to live a dignified life. Every individual lives a life with freedom of life and personal liberty[27]. The person should have complete rights to their personal information, what information should be shared, and whatnot to maintain their privacy. Informational privacy is a facet of the right to privacy: The old adage

[23] Westin, A. F.: Social and political dimensions of privacy. Journal of Social Issues Vol 59, No. 2. (2003) pp. 431.
[24] Gavison, R.: Privacy and the Limits of Law. The Yale Law Journal Vol. 89, No. 3. (1980) p. 423.
[25] Posner, R. A.: The Right of Privacy. Georgia Law Review Vol. 12, No. 3. (1978) p. 393
[26] IJRL, https://ijirl.com/wp-content/uploads/2021/12/ARTICLE-21-A-COMPREHENSIVE-JOURNEY-OF-RIGHT-TO-LIFE-AND-PERSONAL-LIBERTY.pdf (last visited Jan. 20, 2025).
[27] Jordon M. Blanke, Privacy and Outrage, Scholarly Commons (Jan. 20 2025, 8:25 P.M.), https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1110&context=jolti.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

that "knowledge is power" has stark implications for the position of an individual where data is ubiquitous, an all-encompassing presence. Every transaction of an individual user leaves electronic tracks without her knowledge. Individually these information silos may seem inconsequential. In aggregation, information provides a picture of the beings. The challenges that big data poses to privacy emanate from both State and non-state entities. This proposition is described in the following manner.[28]

3.2 Overview of Exiting Data Protection Laws India:

3.2.1 Indian Constitution:

According to Article 21, "No person shall be deprived of his life or personal liberty except according to procedure established by law.[29] Through various case laws, the ambit of Article 21 has been expanded till today. The right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the internet. Needless to say, this would not be an absolute right. The existence of such a right does not imply that a criminal can obliterate his past but that there are variant degrees of mistakes, small and big, and it cannot be said that a person should be profiled to the nth extent for all and sundry to know[30]. Under the right to privacy granted under Article 21, the right to data production is also included, which protects the personal data as the private property of a citizen. Since it is recognized as a fundamental right under Article 21, it cannot be violated except according to the procedure established by law. So, individual data is protected as a fundamental right guaranteed under Article 21.

3.2.2 Indian Contract Act 1872:

Under the Indian Contract Act, when two or more parties form an agreement, they deposit the right to make a confidentiality clause in their contract, which protects the data of these parties. The existence of such a clause will protect and help the parties to keep any private data confidential.

3.2.3 Information Technology Act 2000: The Information Technology Act 2000 was formulated to provide a legal framework to the entire digital ecosystem, which raises privacy:[31]

[28] K. s puutuswamy vs UOI 2019

[29] Yashi Sharma, Right to life and personal liberty under The Constitution of India, E-justice India (Jan. 20 2025, 8:25 P.M.), https://www.ejusticeindia.com/right-to-life-and-personal-liberty-under-the-constitution-of-india/.

[30] Gopal Krishna, Supra Note at 4, at 1993.

[31] Epgp, https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/Law/07._Information_and_communication_technolo

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

There are so many online network platforms where transfer of data is made, which leads to misuse of the database. This act provides a framework to stop the misuse of the data and also establishes heavy penalties to stop cybercrime. Under this act, the one who is using personal information of an individual is obliged to use it with the proper security system so that such data or not misused and no wrongful gain is made to any person. The rules made thereafter under the act also give an obligation to any other to the rules made there under. Such rules state various provisions that regulate the exchange, collection, transfer, and use of private data, making it important to obtain the consent of the individual whose data is used. These provisions help to solve the issue of privacy concerns in the digital era.

3.2.4 Indian Penal Code, 1860:

The offense is given under Indian penal code 1860, due applies only to moving property. It also includes corporeal property of every description, except land and things attached to the earth permanently[32]. Hence, data theft of data constitutes an offense within the meaning of the Indian penal code. As per the provision of the IPC, computer data, personal data, or databases are protected as they are movable in nature.

3.2.5 Copyright act:

The act recognizes computer databases under the definition of literal work, and thereby, it protects such databases amounting to copyright infringement. It also leads down the provisions, penalizing copies of computer databases, giving a legal framework, and protecting the right to privacy of the individual.

3.3 Privacy Risks in this Digital Era:

In the Digital era, along with the advancement of technology, misuse of technology also arises. A few of the risks attached to the misuse of digitalization are as follows. Each issue contributes to the urgent need for data protection laws. The Digital Personal Data Protection Act 2023[33] was introduced to address the rising concerns of privacy and misuse of information in India's rapidly growing digital landscape. The lack of a proper regulatory framework has led to various privacy concerns, which will be discussed below:

gy_/03._Overview_of_Indian_information_technology_act,_2000/et/5741_et_03_ET.pdf (last visited Jan. 20, 2025).

[32] Indian Kanoon, https://indiankanoon.org/doc/1439341/ (last visited Jan. 20, 2025).

[33] Korff D. (2023). The Indian Digital Personal Data Protection Act 2023 is viewed from a European perspective. (Jan. 20, 2025, 8:30 P.M.), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4614984#:~:text=Even%20so%2C%20I%20conclude%20that,have%20to%20adopt%20special%20measures.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

3.3.1 Exchange of information without consent:

One of the major privacy issues is the exchange of personal data without explicitly obtaining the consent of individuals. Many organizations or entities often use the information of an individual without getting clear approval consent from such individuals sensitive personal data, such as financial details, browsing histories, and location are frequently exchanged among entities for commercial purposes without informing the users. For example, many entities who are involved in marketing activities keep records of the data of the individual and exchange it with different entities without informing such individuals that the information is being used for their personal purposes. People are not aware that this information is being recorded and used in the future for any kind of surveillance or marketing purpose the DPDP Act 2023 film mandates such entity is a company to provide explicit consent from the individual before processing or using any such personal data

3.3.2 Unregulated Data Collection:

With the increase in technological advancement, organizations are collecting information without proper regulation. The absence of any string in-laws allows them to use the information in their own way, raising privacy risks. Many abs in website requests are to access the contact list, location, microphone, and camera; even male search does not require further core functionality, users, or individuals who are downloading or using such apps or websites except the terms and conditions, which are notified to them without understanding that they are being dragged by consenting to such terms and conditions in the absence of any regulations or legal framework companies are using personal information and are collecting excessive personal information, which is privacy concerns, the DPDP Act, 2023 enumerates the principle of data minimization, which ensures that organizations or entity should use or collect data which are necessary for their intended purpose.

3.3.3 Cybersecurity threats:

Without a streak to legal framework or regulation, India failed to adopt a digital system that is safe and records for the users. The growing number of cyber-attacks. Hacking incidents run somewhere, and attacks have put everybody at risk in recent years. India has witnessed many such high-profile breaches, such as leaks of Aadhaar details, financial scams, or identity theft, and a lack of robust data, security regulation, or security protocols, resulting in frequent data breaches. The DPDP Act addresses this by mandating strong security measures for data storage and processing. So now companies are mandated to use proper encryption for securing the data,

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

and in case of any breach of, breach, or authorized use of data, it will amount to penalizing as well.

3.3.4 Third-party data sharing:

Many companies involve themselves in sharing the personal information of the individual with advertisers' brokers, rather, businesses, profit, social media platforms, or e-commerce platforms usually exchange their data for their personal purposes, such as targeted advertising or trial or cross-platform profiling. In such a scenario, the individual is not under any control where his or her formation is shared with a third party. A strict regulation or guideline regulating such exchange of information between entities will result in reducing authorized third-party data sharing.[34]

3.3.5 No regulatory framework for curtailing the unauthorized use of personal data:

Before the implementation of the DPDP Act 2023, India lacked in having a proper legal framework for regulating the use of personal data. There were many regulatory frameworks, directly and indirectly, regulating the exchange of personal information, but these frameworks do not establish a strong security protocol for curing the Collection or processing of private data, which are confidential. Due to a lack of clear regulations, businesses frequently engage in unethical data-gathering and sharing methods while operating in a regulatory gray area. People had no legal options in the event that their personal information was exploited, misused, or disclosed. Enforcement was challenging because there was no specific entity in charge of data protection. By creating a precise legal framework for data governance, compliance, and responsibility, the DPDP Act closes this gap. It guarantees that people are protected from data misuse and have access to legal remedies.

3.3.6 Non-Compliance with Global Standards:

India trailed behind in enacting stringent data protection rules as international data privacy regulations changed. Many nations have strict privacy regulations requiring corporations to secure user data, such as the United States (CCPA), the European Union (GDPR), and the United Kingdom (UK Data Protection Act). Non-compliance with global privacy standards made it difficult for Indian corporations to conduct business with foreign companies. India's weak legal system made many international corporations reluctant to exchange or process data there. For its companies to follow worldwide best practices and become more

[34] ET Government, https://government.economictimes.indiatimes.com/news/governance/india-to-play-key-role-in-shaping-global-tech-governance-rules-union-mos-for-external-affairs-rk-ranjan-singh/92585502 (last visited Jan. 20, 2025).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

competitive in the global market, India needed a strong data protection law. The DPDP Act ensures that companies adhere to ethical data practices by bringing India's data protection legislation into compliance with international standards.

CHAPTER 04: THE DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT, 2023:

4.1 Introduction:

The Digital Personal Data Protection Act of 2023[35] establishes a legal framework safeguarding the seamless flow of personal data of the individual. The Digital India initiative has caused digitization across India, particularly in the governance field. The flow of the data to each platform is very easy and accessible to everyone. Presently, internet users are increasing day by day, and this internet and technology is the force for connectivity across the world. Subsequently, it is also a place where the personal data of individuals are misused. The act aims to establish a framework that is fair to each and every individual in such a way that the organizations that are using the data should use the data that are necessary for their purpose, and such use and purpose should be transparent to individuals. The Act also ensures that persons who are using such personal data of the individual are made accountable for processing their data so that individual rights and interests are protected. It aims to establish regulations for the easy transfer of data, obligations for data fiduciaries, and regulations for the processing of such data.

4.2 Formation of The Digital Personal Data Protection (DPDP) Act, 2023:

The government of India, understanding the concern related to data protection, has taken an initiative to ensure the safety and protection of individual's personal data, and the government of India has decided to form a committee under the Chairmanship of former Supreme Court Justice Shri B N Srikrishna which deliberately investigate and suggest on data protection framework for India. The Committee, constituted on 31 July 2017, consisted of experts from different organisations. The main task of the committee was to study different issues related to data protection in India to suggest the government for framing principles and to draft a data protection bill. The Government of India has sought public comments on the data protection framework. The committee has also decided to conduct meetings of different stakeholders for

[35] Nivedita Krishna, THE DIGITAL PERSONAL DATA PROTECTION ACT- AMBIGUITIES, LIMITATIONS AND RECOMMENDATIONS, Wadhwani (Jan. 20, 2025, 8:30 P.M.), https://wadhwanifoundation.org/wp-content/uploads/2024/01/Whitepaper-on-DPDP-Act-and-Rule-Formulation-V-3.0.pdf.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

consultation on framing such principles for data protection in India. After a long process, the Personal Data Protection Bill 2018 was presented in Parliament, and it was reviewed, but it was not passed by Parliament. Later, with a few amendments and changes, a fresh draft was made, i.e., the Digital Personal Data Protection Bill 2022, in November 2022 by the Ministry of Electronics & Information Technology. It was released for public consultation[36]. This freshly drafted bill was presented in the Lok Sabha in August, which led to the foundation for the enforcement of the Digital Personal Data Protection Act of 2023. By using the word "she" instead of "he" for the first time, it acknowledges women in Parliamentary law-making.[37]

4.3 Features of The Digital Personal Data Protection (DPDP) Act, 2023 :

After the enforcement of this act, a legal framework for protecting the interest of an individual in their personal information has been established. Through this act, a clear and precise definition of each term, such as Data, Data Principal, Data Fiduciary, State, Board, Consent Manager, etc. was given. Through this act, the entire processing of digital data was regularised in such a way that all the digital data available should be used only for lawful purposes and with the consent of the Data Principal. Further clarifying the meaning of Data Principal and Data Fiduciary, Data Principal means the one who gave consent to use his or her personal digital data, and Data Fiduciary means the one who uses such data of Data Principal. The data fiduciary can only use the data available to him by the Data Principal under the provisions of the Digital Personal Data Protection Act of 2023[38].

How is the interest of the data principle protected under this act?

1. No information of the Data Principal is used without his or her consent.
2. The Data Principal must have provided his personal data voluntarily.
3. The concern given by the Data Principle must be clear, unconditional, and unambiguous.
4. The personal data of the Data Principal must only be used for that specific purpose for which it was been consented.
5. The Data Principal must be given complete right to withdraw the consent given to the Data Fiduciary.

[36] PSA Legal, https://www.mondaq.com/home/redirect/original/1254806?location=articleoriginal (last visited Jan. 20, 2025).
[37] Arya Tripathi, Digital Personal Data Protection Bill, 2022 – Analysis Of The Key Features, Mondaq (Jan. 20, 2025, 8:40 P.M.), https://www.mondaq.com/india/privacy/1254806/.
[38] Abhishek Chauhan, Why no one is talking? , Linked in (Jan. 20, 2025, 8:45 P.M.), https://www.linkedin.com/pulse/why-one-talking-abhishek-chauhan-maq6f.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

6. In the case where the Data Fiduciary is not able to follow the provisions of this act, then he is subject to compliance against the Data Principal.
7. It is the responsibility of the data fiduciary to maintain reasonable security of the personal data made available by the Data Principal.
8. The Data Fiduciary must establish a redressal mechanism to hear the grievances of the data principal.
9. The Central Government remains a regulatory body to regulate the act of the Data Principal And Data Fiduciary under the provisions of the Digital Personal Data Protection Act of 2023.
10. Under this Data Protection Board of India was created, which performs various functions as below:
    a. When the Board receives any complaint, it should take immediate action to enquire into such matter, and remedy should be provided.
    b. After inquiry, if it feels that there is any breach, then the Board should impose a penalty on such person.
    c. The Board should conduct its inquiry on the basis of the Principle of Natural Justice.
11. If the decision of the Data Protection Board of India is not satisfied, then the aggrieved party can go to an appellate tribunal to get justice. Appellate tribunal will discharge its functions as per the provisions of the act, to solve the problem of the aggrieved and give justice.

4.4 Purpose or Objective of the Digital Personal Data Protection (DPDP) Act, 2023:

1. The main objective of the Data Protection Act is to recognize the rights of the individual to protect personal data.
2. The use of the personal information of an individual can be regularised
3. Misuse of personal information can be prevented by imposing penalties for breach of the rights of an individual.
4. To provide an easy redressal mechanism for solving their complaints regarding unlawful use of personal information.

4.5 Scenario after the DPDP Act,2023

India's data Governance has achieved a significant place through the implementation of the DPDP Act of 2023. The framework of data governance in India has shifted to a significant

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

place where the exchange of personal information of an individual is restricted in a certain way. With the enactment of the Digital Personal Data Protection Act 2023, two features were recognized[39]. Firstly, the right of the individual to protect their personal data and the need to access or process such personal data for lawful purposes only[40]. The act has recognized the right of an individual who is sharing their personal information. The entire processing of the data will be subject to the consent of the data provider. The Data Principal also has the right to withdraw this consent. The information is used to the extent of the consent given. An individual who is sharing such information will have the right to know where is there in information is being shared side this day also has the right to obtain any read for their grievances subject to the use of such data. The data who are using their information are obliged to adhere to the principles or guidelines established by the DPDP Act 2023. Any non-adherence to such principles or provisions will amount to a penalty, as the case may be.

CHAPTER 05: IMPACT OF IMPLEMENTATION OF DPDP ACT, 2023:

The Digital Personal Data Protection, DPDP Act 2023 brings a paradigm shift in how government entities handle personal data that vantages the government entities to regulate the flow of data or data storage or data collection or processing of such data to ensure compliance with the data production principles adopted in this act These principles or regulations include lawful purpose, lawful processing or collection of data. Data security limits the use of data, and many more governments should strictly adhere to the principles of data protection to reduce any kind of privacy violations. While the government also retains certain exemptions in the name of national entrance and interest in security, it is now subject to certain restrictions as well. Public sector organizations must involve data security measures to prevent breaches like the Aadhaar League, enhancing citizen trust in government institutions. The implementation of the DPDP Act 2023 also has a significant impact on businesses and trade, both domestic and international, by enforcing its data protection laws. The digital economy of India is reshaped by implementing these provisions. In the current scenario where it bills. Consumer trust in these businesses, sensitive personal data of the individual is protected through these data, governance policies or provisions which is indirectly gaining a competitive advantage by building cost consumer trust, Businesses failing to comply with these provisions are also facing

[39] Adv. Priyanka, Digital Personal Data Protection Act (DPDPA), 2023, I pleader (Jan. 20, 2025, 8:50 P.M.), https://blog.ipleaders.in/digital-personal-data-protection-act-dpdpa-2023/.
[40] Ibid.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

heavy fines and penalties, pushing them to strictly follow these rules or regulations.[41] The DPDP Act, 2023 is primarily designed to protect individuals' privacy rights guaranteed under Article 21 of the Indian constitution no companies or entities can use their personal information without their consent, establishing a restriction on the authorized use of personal data. This act also established the Data Protection Board of India which will act as a regulatory body through which individuals can seek grizzle for any such privacy violations organizations are required to implement robust security measures, that cities face, lower the risk of identity, theft, financial fraud, cyber-attack and hacking India's DPDP Act, 2023 has implications beyond the national border. It allows cross-border data transfer with certain and restricted data flow for business purposes. Clear data prediction regulations will attract huge foreign investment as well as establish a friendly business environment. The DPDP act alliance with GDPR, general data protection, regulations, and others. Similarly, global privacy loss, positioning India as a privacy-conscious nation, DPDP 2023 is a landmark regulation that transforms India's data privacy framework. It positions India as a key player in global data governance.[42]

CHAPTER 06: CONCLUSION:

6.1 Summary of Key Findings:

India is emerging as a fast-growing nation from the perspective of technological advancement. The a need for proper regulation for the transfer of data across the medium of exchange. The Digital Personal Data Protection Act of 2023 will enhance the regulatory framework for the use of data. The entire research paper focuses misuse of data, raising privacy concerns, and the legal framework established under the act. The implementation of the DPDP Act, 2023, stresses regulating the flow of data across different data fiduciaries so the privacy of the data principal is maintained.

6.2 Key Recommendations:

The implementation of the DPDP Act, 2023 objective of the act can only be achieved if all the data fiduciaries adhere strictly to the provisions of the DPDP Act 2023. The regulators or the competent authorities should act as a watchdog on these data fiduciaries so that any breach of the provisions of the act is avoided. The competent authority should establish

[41] Misra R., & Grover R. (2020). Future of privacy: Evaluating the Personal Data Protection Bill 2019 in light of the contract for the web (Jan. 20, 2025, 8:50 P.M.), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3592363.

[42] DPDPA, https://dpdpa.co.in/wp-content/uploads/2023/08/Data-Protection-Bill-2023.pdf (last visited Jan. 20, 2025).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

clear and detailed guidelines for the organizations using any kind of personal information. The government should invest in awareness programs for any individual who is subject to this provision so that provision enforcement of the act can be obtained. The stakeholders were involved in exchanging. Such information should continuously be made accountable to the competent authorities so that any misuse of information can be cured. It also restricts cross-border data transfer.

www.abhidhvajlawjournal.com
The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.