International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Data Privacy Vis-A-Vis the Digital Personal Data Protection Act, 2023

Jaya Thapa

Assistant Professor (Contractual Basis), GNDUs, RC, Jalandhar

ABSTRACT

The right to privacy is an essential human entitlement that involves an individual's independence and authority over their personal data. In an era dominated by digital interactions and data-driven technologies, the right to privacy has become increasingly pertinent. The concept of data privacy encompasses the protection of personal information from unauthorized access, use, and disclosure. With the proliferation of online platforms and digital services, individuals are generating vast amounts of data, raising concerns about its misuse and exploitation. Data privacy in India has become a significant issue with the increasing digitization of services and the proliferation of personal data collection by both government and private entities. In 2023, the digital data protection act was enacted to specifically deal with Data privacy as well as Data protection.

This paper attempts to analyse the right to privacy vis-à-vis the digital data protection act, 2023 and this analysis explores how these regulatory provisions address the emerging challenges to the protection of sensitive personal data.

Keywords: Data Privacy, Right to privacy, Data Protection

I. INTRODUCTION

Around the world, privacy has come to be seen as a fundamental human right; in India, it is officially recognised as such under Article 21 of the Indian Constitution. The right to privacy is intimately linked to data protection, which is more challenging to accomplish in today's technologically advanced and international society. Furthermore, because this right is not legally protected, it is now conceivable for the ruling majority to violate private rights through discriminatory legislation.

This right was not originally acknowledged as a Fundamental Right in India, and no particular data protection legislation was passed to safeguard citizens' rights to privacy. Simultaneously, there have been several accusations of privacy rights violations in India, made by both the government and private commercial entities on occasion. These accusations were also brought before the legal courts, which rendered historic decisions that included guidelines and verdicts.

These days, it is reported that public employees are threatening privacy under the guise of "public duty" or "procedure established by law," which is perhaps the most important factor in human life on Earth. Let us ponder for a moment what would happen to an individual in the event that they were to be deprived of their right to privacy, which encompasses all private rights related to relationships, family, employment, and other areas. In a literal sense, privacy is as essential to human health as air is. It is the means by which our Indian Constitution's Article 21 guarantees a life of peace, dignity, and liberty. With the increasing use of social media and the Internet in many fields, it is appropriate to refer to this period as the "Cyber

Era" as our nation gradually moves towards digitalization. Data security and protection, which are essential components of privacy as your digital footprint, are both national issues and obligations that must be met. Data protection and privacy are closely related and currently occupy one of the most sensitive and important legal spaces.

II. RIGHT TO PRIVACY AND DATA PROTECTION

One of the primary factors that necessitated the evolution of privacy rights was the need to safeguard and preserve the dignity of an individual and consequently preventing unauthorized disclosure of personal information in the public domain. But with the advent of the digital age, the scale of data produced and used have changed drastically. The manner in which the digital revolution impacts privacy, particularly the concerns with regard to the misuse and manipulation of personal information, has also given rise to the concept of informational privacy.[1]The right to privacy is an individual entitlement bestowed by objective legal frameworks. Constitutional law, prominently featuring provisions safeguarding citizens from excessive state intrusion, notably exemplifies how this subjective right is legally recognized. Although the right to privacy is not specifically mentioned in the Indian Constitution, Indian courts have addressed the issue of whether or not it is a basic right in India. The case of *M.P Sharma v. Satish Chandra*[2], A landmark decision by an eight-judge bench of the Supreme Court addressed issues concerning the validity of a search warrant issued under Section 96(1) of the Criminal Procedure Code, 1973. It marked the inaugural case to explore matters pertaining to privacy. In that case, the Apex Court ruled that the Indian Constitution did not provide the basic right to privacy. This position was reiterated in *Kharak Singh v. State of Uttar Pradesh*[3]. However, cases such as *PUCL v. Union of India*[4], it was held violation of right of privacy include telephone tapping. In *Selvi v. State of Karnataka* [5], which declared in order to avoid violating an individual's confidentiality, investigative methods such as polygraphs, narco-analyses, and BEAP have been used without that person's prior agreement. This has raised questions about whether the Constitution protects the right to privacy.[6]

Finally, a larger Bench of the Supreme Court had the opportunity to address this question in *K.S Puttaswamy v. Union of India*[7]. The background of this case was Aadhar, the Indian government's biometric identity scheme. In this instance, the argument that Aadhaar infringed upon an individual's right to privacy was used to contest the constitutionality of the system. According to Chandrachud J., the right to privacy is a fundamental inherent right and a component of human dignity. In addition, he discussed the need of privacy in the digital economy, informational privacy, and the necessity of a data protection legislation.[8]

The technology and law are inter-dependent on each other, and this will surely witness an active increment in future, according to a Research, the advance time of law will surely be based purely on Artificial Intelligence (AI), which will bring more new challenges and impediments in the way of Right to Privacy and Data Protection in India as well as the World. We can see that how the technology can infringe your

[1] Payal Thaorey, "Informational Privacy: Legal Introspection in India" 2 *ILI Law Review* 166 (2019).
[2] AIR 1954 SC 300
[3] (1964) 1 SCR 332
[4] AIR 1997 SC 568,
[5] 2010 SC 1974
[6] SHIVANI JOSHI, *DATA PROTECTION IN INDIA: A COMPARATIVE STUDY (*2019) (Unpublished Ph.D. thesis, Institute of Law Nirma University Ahmedabad).
[7] (2017) 10 SCC 1
[8] Ibid.

Privacy and can create blunders in your life, the investigating agencies can revive your all the deleted chats, messages and recordings from stored backup for the purpose of law which is known as "Digital Footprint" of any time, and it is regarded as the exact replica of the individual on the servers.[9]

Data protection and the Right to privacy have become crucial issues in today's digital world. With the increasing use of technology, forms of data have diversified, making it more challenging to ensure adequate protection for personal information. It also underscores the need for robust data protection measures that can effectively safeguard sensitive information against misuse, theft, or unauthorized access by malicious actors online. From our personal information, financial records, and even medical history, a vast amount of sensitive data is being generated and processed every single day. However, with this abundance of data comes the need for effective protection measures to ensure privacy and prevent unauthorized access or misuse.[10]

In recent years, there has been an increasing concern regarding the security of sensitive data due to high-profile breaches that have exposed millions of people's personal information. This has led to a growing awareness of the importance of protecting sensitive data from cyber threats such as hacking, identity theft, and phishing attacks. Data protection and data privacy is also been misunderstood in the term of privacy. However, Data protection and data privacy are totally different in nature.[11]

III. LEGAL FRAMEWORK FOR PROTECTION OF DATA IN INDIA

In India, while the terms "Privacy" and "Data Protection" are not explicitly defined in legal statutes, their scope is covered comprehensively by various laws. The Constitution of India, particularly Article 21, guarantees the fundamental right to life and personal liberty, which has been interpreted by the Supreme Court to include the right to privacy and protection of personal data. The Indian Penal Code of 1860 addresses offenses like voyeurism, stalking, theft of data, extortion, and forgery, providing penalties for violations that infringe upon privacy. The Information Technology Act of 2000 specifically deals with cybercrimes, including hacking, password fraud, violation of privacy through unauthorized capture or transmission of images, and publishing obscene or sexually explicit material online. Additionally, the Copyright Act of 1957 protects intellectual property rights, which indirectly safeguards creators' privacy by regulating unauthorized use of their works. The Indian Contract Act of 1872 governs contractual agreements, allowing parties to include clauses that protect privacy and data rights. Together, these legal frameworks aim to ensure individuals' privacy and data are respected and protected under Indian law, with provisions for both civil and criminal remedies against violations.[12]

The term "Privacy" and "Data Protection" are nowhere defined in any of the Statute, Law, Order or Notification, but the scope and ambit of our Constitution of India and various other Statutes are wide enough to cover the Privacy and Data Protection under it. The Laws governing the same are as follows:

1. Constitution of India: The Article 21 i.e. Protection of Life and Personal Liberty which states that "*No Person shall be deprived of his life or personal liberty except according to procedure established by law*", even the Preamble of India ensures the Liberty of thought, expression, belief, faith and worship to all its citizens, which covers the individual's right of privacy under it's ambit to rule and govern and provide

[9] Neelam Rai, "Right to Privacy and Data Protection in the Digital Age – Preservation, Control and Implementation of Laws in India" 11 *IJLJ* 115 (2017).
[10] *Supra* note 10.
[11] *Ibid.*
[12] Kuldeep Yadav, "Right to Privacy and Data Protection Under Indian Legal Regime" 8 *International Journal of Law* 134 (2022).

justice on violation of the same. In 2017, the Honourable Supreme Court of India declared that the right to privacy is a fundamental right, encompassing the idea of data protection, since any threat or unauthorised access to an individual's data without that individual's express consent amounts to a clear and present violation of that right. The court based this decision on the word "liberty" appearing in both the Preamble and Article 21. [13]

2. Indian Penal Code, 1860- The Indian Penal Code, a cornerstone of India's criminal law, addresses several offenses pertinent to privacy and data protection. Section 354-C criminalizes voyeurism, punishing those who capture and publish images of women engaged in private acts with imprisonment ranging from one to seven years. Section 354-D deals with stalking, penalizing individuals who follow women without consent, causing mental distress, with up to five years' imprisonment and a fine. Section 379 covers theft of private data, penalizing illegal access or copying with imprisonment or fines. Section 383 addresses extortion involving private documents or data, punishable with up to three years' imprisonment or fines. Finally, Section 471 penalizes the use of forged documents or electronic records that infringe on privacy or data protection with imprisonment of up to two years or fines. These provisions collectively aim to safeguard privacy and deter offenses against personal data in India.[14]

3. Information and Technology Act, 2000: The Information Technology Act, 2000 focuses on combating cybercrimes and protecting data privacy. Section 66 addresses hacking, penalizing unauthorized access to computer resources with up to three years' imprisonment, a fine up to five lakh rupees, or both. Section 66C targets password fraud, punishing the unauthorized use of passwords with imprisonment up to three years or fines up to one lakh rupees. Section 66E addresses privacy violations, penalizing the unauthorized capture or transmission of a person's image with up to three years' imprisonment or fines up to two lakh rupees. Sections 67 and 67A deal with the publication or transmission of obscene or sexually explicit material online, punishable with imprisonment ranging from three to seven years and fines up to ten lakh rupees. These provisions collectively aim to safeguard data integrity and privacy in India's digital landscape.[15]

4. Copyright Act, 1857: Although the Act was passed prior to independence, it substantially safeguards the creator's intellectual property rights now that it has been incorporated into our legal framework. It primarily safeguards the author's creative works—literary, dramatic, musical, and artistic—during their lifetime and for 60 years following their passing. If anyone copies, replicate or uses the creation of the author, without his explicit permission for some commercial gain or some other use which includes publishing, circulating or transmitting, so for such infringement of the private rights of the author, the Act, provides Civil as well as Criminal Remedies, in former, the victim can seek or plead for Injunctions and Damages from the tortfeaser, and in latter the punishment if found guilty includes imprisonment up to Three years and fine up to Rupees Two Lacs.[16]

5. Credit Information Companies Regulation Act, 2005("CICRA")

The Credit Information Companies Regulation Act, 2005 (CICRA) in India primarily regulates credit information bureaus that collect and maintain credit-related information on individuals and businesses. While CICRA itself does not explicitly focus on data privacy in the broader sense, it indirectly impacts

[13] Jayanta Ghosh and Uday Shankar, "Privacy and Data Protection Laws in India: A Rightbased Analysis" *Bharati Law Review* 59 (2016).
[14] *Ibid.*
[15] Syamantak Sen and Antra Sisodiya, "An Analysis of Data Protection Laws in India" *The World Journal on Juristic Polity* 2 (2017).
[16] *Ibid.*

data privacy by governing how credit information can be collected, stored, and shared by credit bureaus. Under CICRA, credit information companies (CICs) are mandated to handle sensitive financial data responsibly. They must ensure the accuracy, confidentiality, and security of the information they collect. This involves maintaining robust data protection practices to prevent unauthorized access, misuse, or disclosure of sensitive personal information.[17]

Moreover, the Act stipulates that individuals have the right to access their credit information and correct any inaccuracies. This provision aligns with principles of data privacy, ensuring individuals have some control over their financial data.

IV. THE SALIENT FEATURES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

1. History

There is a recent act passed for data processing in India i.e **The Digital Personal Data Protection Act, 2023.** It was finally adopted almost six years after the Supreme Court recognised the fundamental right to privacy in Article 21after *Puttaswamy case* [18] when the Govt. of India has set up a committee of five members headed by former Supreme Court judge, Justice (Retd.) B.N. Srikrishna for drafting a Data Protection Bill. It came in July 2018- the Personal Data Protection Bill, 2018. However, it was withdrawn in August 2022 due to numerous recommendations for amendments presented by a Joint Parliamentary Committee, which submitted its report in December 2021. The Digital Personal Data Protection Bill, 2022 (DPDP Bill) was drafted by the Ministry of Electronics and Information Technology (MeitY) on November 18, 2022. On August 11, 2023, the bill became an Act.[19] The purpose of this act is to process and protect the personal data in India.[20]

2. DEFINITIONS AND APPLICABILITY

Some definitions are discussed below:

1. The representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by human beings or automated means is often referred to as "data." [21];
2. A data fiduciary is any individual or entity that independently or jointly with others determines the purposes and means of processing personal data [22];
3. The individual to whom personal data relates. If the individual is a child, the definition includes their parents or lawful guardian. If the individual is disabled, it includes their lawful guardian[23];
4. Data Processor is any person or entity that processes personal data on behalf of a Data Fiduciary[24]
5. Personal data refers to any information that relates to an identified or identifiable individual[25]

The act is applied to the processing of digital personal data within the territory of India where the personal data is collected (i) in digital form; or (ii) in non-digital form and digitised subsequently and outside the

[17] *Ibid.*
[18] Pradip Kumar Kashyap, "Digital Personal Data Protection Act, 2023: A New Light into the Data Protection and Privacy Law in India" 2 *Icrep Journal of Interdisciplinary Studies* 7 (2023).
[19] *Ibid*
[20] *Ibid*
[21] The Digital Personal Data Protection Act, 2023 (NO. 22 OF 2023), s. 2(h).
[22] *Id.*, s. 2(i).
[23] *Id.*, s. 2(j).
[24] *Id.*, s. 2(k).
[25] *Id.*, s. 2(t).

territory of India, the activity related to offering of goods or services to Data Principals within the territory of India. This act do not apply to personal data processed by an individual for any personal or domestic purpose; and it is publicly available by (A) the Data Principal to whom such personal data relates; or (B) any other person who is under an obligation under any law in India.[26]

3. OBLIGATIONS OF DATA FIDUCIARY

There are some obligations on the data fiduciary under the act. According to section 4, the personal data may be processed only in accordance with the provisions of this Act and for a lawful purpose. It is important to take consent and use it for legitimate purposes.

The legitimate uses can be (a) the Data Principal gave its personal data voluntarily and not using it without consent. (b)Where any subsidy, benefit, service, certificate, licence or permit is to given by the state or any instrumentalities then consent regarding it (c) in the interest of sovereignty and integrity of India or security of the State.(d) for the purpose of satisfying any legal requirement that is now in effect in India for someone to provide information to the State or any of its agencies.

(e) any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India (f) medical emergency involving a threat to the life or immediate threat to the health[27](g) for taking measures to provide medical treatment during an epidemic, outbreak of disease, during any disaster, or any breakdown of public order. (h) to the extent necessary to fulfil employment obligations or protect the employer against harm, including but not limited to preventing corporate espionage, maintaining trade secret and intellectual property confidentiality, providing any service or benefit requested by an employee of the Data Principal, or providing classified information.[28]

NOTICE -The prerequisite of processing the data is the notice given to the Data Principal stating the concerned data, the purpose of processing, rights and manner in which complaint can be done by Data Principal[29]. In cases where a data principal has consented to the processing of her personal data prior to the Act's commence, it is also applicable; however, the data principal's consent may only be processed up to and unless she withdraws it[30].

CONSENT- The consent of Data Principal should be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and with an agreement which specify the specified purpose and then limiting to the said purpose.[31] If any part of consent is against the act or rules then it shall be invalid. Plain and clear language should be used and also the contact of a Data Protection Officer or any other authorised person to be given. Consent can be withdrawn at any time but the consequences shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal[32]. Once consent is withdrawn, processing must stop unless processing is allowed under the act or rules or any other law for the time being in force in India. The consent manager, registered with the board, can be kept by Data principal who act on her behalf. The burden of proving on the question of consent lies on the Data Fiduciary that consent was taken according to the act and rules.[33]

[26] *Id.*, s. 3.
[27] The Digital Personal Data Protection Act, 2023 (NO. 22 OF 2023), s. 7.
[28] *Ibid.*
[29] *Id.*, s. 5(1).
[30] *Id.*, s. 5(2).
[31] Graham Greenleaf, "India's 2023 Data Privacy Act: Business/Government Friendly, Consumer Hostile" 3 (2023)
[32] *Supra* note 29, s. 6.
[33] *Supra* note 29, s. 6.

There are general obligations of Data fiduciary mentioned under section 8 of this act. Data fiduciary must

1. carry out its duties mentioned under the act
2. may engage, appoint, use or otherwise involve Data Processor
3. ensure the data shall be complete, accurate and consistent as it is used to make a decision and even disclosed to another Data Fiduciary
4. implement technical and organisational measures
5. Protect data under its possession and control by implementing reasonable safeguards.
6. intimating the board about any data breach
7. erase personal data when consent withdrawn and also causes its data processors to do so
8. publish the business contact information of Data Protection offices
9. establish an effective mechanism for the redressal of grievances.[34]

CHILDREN - Before processing the personal data of child or disabled person, consent from parent or lawful guardian must be obtained. Anything which have detriment effect on the well-being or tracking or behavioural monitoring is not allowed.[35]

SIGNIFICANT DATA FIDUCIARY - The Central Government may notify the Significant Data Fiduciary (herein after referred as SDF), on the basis of some factors such as the volume and sensitivity of personal data processed, risk to the Data Principal's rights, impact on the sovereignty and integrity of India, risk to electoral democracy, security of the State and public order. Data Protection Officers and independent data auditor should be appointed[36].

4. RIGHTS AND DUTIES OF DATA PRINCIPAL

a. The Data Principal can obtain the information from Data Fiduciary regarding: (i) summary of personal data processed and processing activities. (ii) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared and the description of data shared. (iii) any other information. There is an exception that no such information of the data fiduciary is to be given if Data Fiduciary authorised by law and sharing is for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.[37]

b. Right to correction and erasure of personal data- A Data Principal shall send a request for correction, completion or updating of data-to-Data Fiduciary. Data Principal can also erase the personal data by requesting and it shall be erased by the Data Fiduciary. [38]

c. Right of grievance redressal -A Data Principal shall have the right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager. When addressing the Board, the Data Principal must first use this section's grievance resolution process.[39]

d. The principal may designate another person to represent him in the event of his death or incapacity[40]

e. Duties of Data Principal- The data principal must comply with the provisions of all applicable laws while exercising the rights. There must be no impersonation while providing personal data and no

[34] *Id.*, s. 8.
[35] *Id.*, s. 9.
[36] *Id.*, s. 10.
[37] *Supra* note 29, s. 11.
[38] *Id.*, s. 12.
[39] *Id.*, s. 13.
[40] *Id.*, s. 14.

suppression of material information. No false or frivolous complaint should be registered. While exercising the right to correction or erasure, must only give verifiably authentic information.[41]

5. DATA PROTECTION BOARD OF INDIA

The data protection board of India is established under this act. It consists of a chairperson and such number of other Members as the Central Government may notify. The appointment, salary, allowances and other terms and conditions of service of the Chairperson and other Members. The Chairperson and the other Members are eligible for reappointment after serving two-year terms in office.[42]

The Board shall exercise and perform the powers and functions as given under the act[43]. The intimation of breach of data can be received by Data Principal in the form of complaint or on reference by the central government, the board should inquire into such breach and impose penalty as provided in this Act. The Board may modify, suspend, withdraw or cancel direction. It is an independent body and shall function as a digital office, with the receipt of complaints and the allocation, hearing and pronouncement of decisions in respect of the same being digital by design, and adopt such techno-legal measures. Reasons must be recorded either to proceed with inquiry or, close the proceedings.[44]

6. APPEAL AND ALTERNATE DISPUTE RESOLUTION

According to section 29 of the act, any individual affected by an order or directive issued by the Board has the right to appeal to the Appellate Tribunal. The appeal must be submitted within sixty days from receiving the order or directive, unless there are valid reasons for a delay which satisfy the Tribunal. Every order issued by the Appellate Tribunal must be copied to both the Board and the appeal's parties. Within six months of the appeal being submitted to it, it must render a final decision on it. If the appeal is not filed within six months, the reasons must be documented in writing. In cases where an appeal is lodged against the decisions of the Appellate Tribunal under this Act, the provisions of section 18 of the Telecom Regulatory Authority of India Act, 1997, shall be applicable.[45]. An order issued by the Appellate Tribunal under this Act can be enforced by the Tribunal itself as if it were a decree of a civil court. For this purpose, the Appellate Tribunal possesses all the powers vested in a civil court.[46]

There is a special provision of mediation, where the board can direct the parties concerned to resolve their dispute by mediation.[47] The voluntary undertaking may be accepted by the Board for the observance of the provisions of this Act from any person at any stage of a proceeding. The Board has the authority to modify the terms of a voluntary commitment upon acceptance, with the consent of the individual who submitted it. Once accepted by the Board, a voluntary commitment prevents any proceedings under this Act regarding its contents. However, if a person fails to comply with any term of the accepted voluntary commitment, this breach will be treated as a violation of the provisions of this Act. The Board may impose penalties after providing the person with an opportunity to be heard.[48]

7. PENALTIES AND ADJUDICATION

The board can impose monetary penalty when there is breach of the provisions of the act. The amount of that penalty depends on (a) the nature, gravity and duration of the breach; (b) the type and nature of the

[41] *Id.*, s. 15.
[42] *Supra* note 29, s. 19.
[43] *Id.*, s. 27.
[44] *Id.*, s. 28.
[45] *Id.*, s. 29.
[46] *Id.*, s. 30.
[47] *Id.*, s. 31.
[48] *Id.*, s. 32.

personal data affected by the breach; (c) repetitive nature of the breach; (d) if the individual has achieved a benefit or averted any loss as a result of the violation; (e) whether or whether the individual took any effort to lessen the impact of the breach, and if so, when and how well it worked; (f) whether the proposed financial punishment is reasonable and appropriate in light of the requirement to ensure that the Act's provisions are followed and to discourage violating them; and (g) the probable effects of the financial penalty being imposed on the individual.[49]

V. LOOPHOLES IN THE ACT

There are some loopholes which are mentioned below**:**

- The DPDP Act won't become fully apparent until the regulations are published, the Board is constituted, and it begins interpreting and enforcing the new law's principle-based requirements. [50]
- There is lack of proper procedures for creating processing and transmitting and flowing of Information.
- Despite having a distinct provision for data transfer, the DPDP Act does little to safeguard the data against potential breaches at the time of transfer. Entities outside of India that keep an eye on the actions of data subjects within India are exempt from the DPDP Act.
- All forms of digital personal data fall under the uniform application of the DPDP Act. No further safeguards are in place for processing important personal data—which was previously suggested—or sensitive personal data, as defined by the SPDI Rules. Although consumers may like to be notified of the breach, it is unclear whether it is necessary to notify of all personal data breaches without any threshold. Notifying people about every personal data breach might lead to information overload and unwarranted concern. Individual notification can also be expensive, both in terms of initial notice distribution and follow-up correspondence with impacted data principals.
- The DPDP Act does not specify a maximum penalty for multiple breaches, such as failing to implement reasonable security safeguards and failing to notify the Board of a data breach. Instead, it imposes penalties for each individual offense, which may be aggregated to determine the maximum penalty applicable.
- Significant exclusions from the DPDP Act are available to the government and other government instrumentalities, providing them with unfettered and unchecked ability to collect and handle data. These exemptions are not limited to start-ups promoting innovation and growth. It restricts information access as defined by the Right to Information Act. Personal information is excluded from disclosure under Section 8 of the RTI Act if it has no connection to public activities. On the other hand, the DPDP Act prohibits the dissemination of any personal data. This strikes at the fundamental foundation of the system's accountability and openness.
- The Act specifies that the Central Government may impose restrictions on cross-border transfers. Using this method, the Act does not adequately secure an individual's personal information.
- The Act also addressed the important question of the Data Protection Board's independence. Although the Act declares it to be an independent body, it is difficult to assume that the board would be autonomous given the tenure of the appointment and the involvement of the government in its operation.

[49] *Id.*, s. 33.
[50]

- The effectiveness of the DPDP Act hinges on public awareness of their rights and responsibilities regarding personal data. It is crucial for individuals to understand how their personal information is collected, processed, and how they can address any concerns they may have. Despite being a recent addition to India's privacy laws, many people remain unaware of its existence and operational mechanisms. The legislation currently lacks provisions mandating the Government or the Data Protection Board to actively educate the public about their data rights and protections.

An important development in the fight to protect our right to privacy is the DPDP Act. It fills up the enormous gap that was present before to the Act. Its extensive provisions show that a real effort has been made to meet the escalating issues of the digital era. As mentioned previously, the Act contains some encouraging aspects. There are undoubtedly certain issues with the Act as well. Fairness issues are raised by the Act's restriction to digital data alone, lack of differentiation between data types, and exemption of the government from its application.

VI. CONCLUSION

In conclusion, India's data privacy and protection laws are a reflection of the world at large as data is becoming increasingly important in the sophisticated digital era. The DPDP Act's adoption is a positive step towards safeguarding personal information, giving data principals more control over their data, and establishing responsibility for data protection agencies. The Act emphasises the rights of Data Principals and highlights important concepts such purpose limitation, accuracy, responsibility, and data minimization. It monitors how Data Fiduciaries carry out their responsibilities and levies fines for breaking rules. The DPDP Act as a whole accomplishes the goals for which it was designed, yet it is not impervious to criticism. The original bill's sensitive personal data protections have been removed, turning it into an Act. Many argue that the DPDP Act is essentially a lost opportunity since it is vague about how permission is obtained, how data is used, and it gives the government broad exemptions. The Act is anticipated to strike a delicate balance between its accomplishments and criticisms while upholding the principles outlined in the Supreme Court's privacy judgement.