Legal Issues in the Digital Age. 2025. Vol. 6, no. 2.
Вопросы права в цифровую эпоху. 2025. Том 6. № 2.

IT. Law. Human Rights

Research article
JEL: K1
UDK: 342.7
DOI:10.17323/2713-2749.2025.2.87.117

Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023

Usha Tandon[1], Neeral Kumar Gupta[2]

[1] Dr. Rajendra Prasad National Law University, Prayagraj, Uttar Pradesh 211013, India,

vc@rpnlup.ac.in;utandon26@gmail.com, https://www.rpnlup.ac.in/

[2] Institute of Law, Nirma University, Ahmedabad, Gujarat 382481, India,

neeraj_6336700@yahoo.co.in, https://law.nirmauni.ac.in/ India

Abstract

Informational privacy, often referred as data privacy or data protection, is about an individual's right to control how their personal information is collected, used and shared. Recent AI developments around the world have engulfed the world in its charm. Indian population, as well, is living under the cyber-revolution. India is gradually becoming dependent on technology for majority of the services obtained in daily life. Use of internet and Internet of Things leave traces of digital footprints which generate big data. This data can be personal as well as non-personal in nature. Such data about individuals can be utilised for understanding the socio-economic profile, culture, life-style, and personal information, like love life, health, well-being, sexual preferences, sexual orientation and various other types of individual traits. Issues like data breach, however, have also exposed users of information and technology to various types of risks such as cyber-crimes and other fraudulent practices. This article critically analysis recently enacted Digital Personal Data Protection Act, 2023 (DPDP) in the light of following questions: How it tackles with the issues of informational privacy and data processing? What measures have been envisaged under the DPDP Act, for the protection of informational privacy? How individual rights with respect to data protection

are balanced against the legitimate state interest in ensuring safety and security of the nation? Whether this right is available only against the State or against the non-State actors as well? etc. Having critically analysed DPDP Act, the article calls for further refinement of DPDP Act in various areas, more specifically, suggesting that, it is imperative that DPDP Act requires critical decisions based on personal data to undergo human review, ensuring they are not solely the result of automated data processing.

Keywords

privacy; data; technology, governance; DPDP Act; AI.

For citation: Tandon U., Gupta N.K. (2025) International Privacy in the Age of Artificial Intelligence: Critical Analysis of India's DPDP Act 2023. *Legal Issues in the Digital Age,* vol. 6, no. 2, pp. 87–117. DOI:10.17323/ 2713-2749.2025.2.87.117

Introduction

India is the largest country in terms of population, and if it is compared with some of the European countries, it may accommodate many such countries. India is also the biggest democracy thriving in the world working towards the material and spiritual well-being of its citizens. Indian population and its rate of consumption has been the hallmark of India's growth in last few decades. Therefore, businesses, and corporations see India as one of the biggest markets. The rate of consumption in every sector has been unprecedented, especially the mobile and internet usage. Today, a large population is using mobile connections as well as Internet services.[1] The volume of Internet data being consumed and number of mobile and internet users reveal there is an increasing trend towards digitalisation.[2]

It is estimated that India's E-commerce industry is worth 125 billion US$ and it is expected to reach 345 billion US$ by financial year 2030. Another estimation provides by the end of 2025 India will have 200 million e-commerce consumers. Further, India's digital banking revolu-

[1] It is estimated that around 102 billing mobile connections were active in the year 2024, 806 million individualsare using the internet. Along with it, there are around 491 million social media users in the country. See Data Reportal, "Digital 2025: India" Feb 25, 2025, available at: https://datareportal.com/reports/digital-2025-india (accessed: 14 April 2025)

[2] Ray Le Maistre, "India now has 1.15 billion mobile connections", *Access Evolution,* Jan 12, 2024, available at: https://www.telecomtv.com/content/access-evolution/india-now-has-1-15-billion-mobile-connections-49371/ (accessed: 19 May 2025)

tion along with UPI is being accessed by 350 million users. A large network of interconnected network of 550 banks is working in the country with the help of 77 mobile applications. Around 2.19 trillion dollars' worth transactions were carried out in India with the help of UPI.[3] It is also to be noted India has world's largest Unique Identification System (UIDAI) where biometric identity in the form of fingerprints and iris scan of 1.38 billion is captured and stored in digital form.[4]

These numbers are sufficient to indicate that India is living in the era of digital revolution. However, the picture narrated above is just the half of the story. Use of digital technology and digital processes have posed various challenges in recent past. India has faced many instances of data breach where data of individuals stood compromised. Some of the major examples of data breach include breach of credit and debit card user's data,[5] LPG consumer's data,[6] *AADHAR* data.[7] Further, data breach in the State Bank of India,[8] and Kudankulam nuclear power plant's data breach,[9] and many more instances highlight that data breach may be a

[3] Ritesh Shukla, "UPI: revolutionising real-time digital payments in India" June 26, 2024, available at: https://www.europeanpaymentscouncil.eu/news-insights/insight/upi-revolutionising-real-time-digital-payments-india#:~:text=How%20many%20users%20and%20payment,in%20a%20seamless%20digital%20manner (accessed: 19 May 2025)

[4] Unique Identification Authority of India. Government of India. About UIDAI, available at: https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india.html#:~:text=About%20UIDAI&text=The%20UID%20had%20to%20be,to%20the%20residents%20of%20India (accessed: 19 May 2025)

[5] Anshika Kayastha, ICICI Bank blocks 17,000 credit cards after data breach. The Hindu Business Line, April 26, 2024, available at: https://www.thehindubusinessline.com/money-and-banking/icici-bank-blocks-17000-credit-cards-after-data-breach/article68109673.ece, (accessed: 19 May 2025)

[6] Business Standard, "Top LPG supplier leaked millions of Aadhaar data: Security researcher", Feb 19, 2019, available at: https://www.business-standard.com/article/news-ians/indane-leaked-millions-of-aadhaar-numbers-french-security-researcher-119021900172_1.html, (accessed: 19 May 2025)

[7] Nabeel Ahmed, "How the personal data of 815 million Indians got breached | Explained" *The Hindu*, November 07, 2023, available at: https://www.thehindu.com/sci-tech/technology/how-the-personal-data-of-815-million-indians-got-breached-explained/article67505760.ece, (accessed: 19 May 2025)

[8] Udit Verma, "SBI data leak: What happened? What can you do? All you need to know" *Business Today*, available at: https://www.businesstoday.in/technology/story/sbi-data-leak-what-happened-sbi-data-breach-financial-data-168220-2019-02-01, (accessed: 19 May 2025)

[9] Nirmal John, "Breach at Kudankulam nuclear plant may have gone undetected for over six months: Group-IB", *Economic Times*, Nov 25, 2020, available at:

national security concern. Furthermore, usage of mobile and internet services for banking purposes has led to rise in cases of digital financial frauds. Number of such cases have increased massively in last decade.[10] Such shocking instances severely impact the lives of the victims of such frauds.[11] Additionally, recent issues of deepfake images and voice cloning with the help of Artificial Intelligence (hereinafter as AI) have led to various types of frauds and embarrassing situation in many cases.[12]

In background, the article contain critical analysis recently enacted Digital Personal Data Protection Act, 2023 in the light of following questions: How it tackles with the issues of data privacy and data processing in the era of AI? How right to privacy, especially, informational privacy, may be protected in the technological era? Whether such right is available only against the State or against the non-State actors as well? What measures have been envisaged under the DPDP Act, for the protection of personal data? How individual rights with respect to data protection are balanced against the legitimate State interest in ensuring safety and security of the nation? etc.

The article is divided into six parts including Introduction and Conclusions. Dealing with the evolution of the right to informational privacy in India, it analyses the judgment of *Puttaswamy* case[13]. It proceeds to discusses the relevant provisions on informational privacy from the IT Act, 2000. The next pages contain the critical analysis of recently enacted data protection law *viz*. the Digital Personal Data Protection Act, 2023 (DPDP Act) in the context of AI. Last part deals with conclu-

---

https://economictimes.indiatimes.com/news/politics-and-nation/breach-at-kudankulam-nuclear-plant-may-have-gone-undetected-for-over-six-months-group-ib/articleshow/79412969.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (accessed: 19 May 2025)

[10] India loses 107 crore to cyber fraud in the first three quarters of this fiscal, https://www.cnbctv18.com/business/finance/india-cyber-fraud-digital-payments-losses-rs-107-crore-fy25-19571280.html (accessed: 20 April 2025)

[11] Pavneet Singh Chadha, "A reclusive couple and a double suicide — Karnataka village wakes up to fallout of digital fraud", *The Indian Express,* April 11, 2025, available at: https://indianexpress.com/article/long-reads/a-reclusive-couple-and-a-double-suicide-karnataka-village-wakes-up-to-fallout-of-digital-fraud-9937402/ (accessed: 19 May 2025)

[12] Pankaj Mishra, "AI Scams Surge: Voice Cloning and Deepfake Threats Sweep India", *NDTV AI*, Oct 10, 2024, available at: https://www.ndtv.com/ai/ai-scams-surge-voice-cloning-and-deepfake-threats-sweep-india-6759260 (accessed: 19 May 2025)

[13] *Justice K. S. Puttaswamy (Retired.) And Anr.* v. *Union of India and Ors.* (2017) 10 SCC 1.

sion and suggestions calling for the further enhancement of DPDP Act, with special focus on the suggestion that DPDP Act must incorporate provisions mandating that consequential decisions derived from data analytics be subject to human oversight, rather than relying exclusively on algorithmic outputs.

1. Evolution of the Right to Informational Privacy in India: *Puttaswamy* Judgment

In simple words informational privacy, that's an emerging phenomenon and often referred as data privacy or data protection is about an individual's right to control how their personal information is collected, used and shared. The concept of informational privacy stems from the right to privacy. In India the questions relating to right to privacy have been the matter of concern since its independence. Concerns for privacy were raised in the Constitutional Assembly Debates. It was argued that privacy of correspondence must be included expressly in the Constitution of India.[14] Also, it was proposed that there should be express provision recognizing protection from the unwarranted and intrusive searches and seizure by the State as provided in the American Constitution.[15] However, the final text of the Constitution of India[16] did not contain any express provision with respect to right to privacy.

Issues of unreasonable searches, seizure and State surveillance by the State came to be argued in Supreme Court in 1954[17] and 1964.[18] These cases held that searches and seizure by State are not protected by right to privacy as the same is not expressly recognised under the Indian Constitution. It is interesting to note: the case of *Kharak Singh* regarded the sanctity of home and privacy as a facet of liberty but ironically has failed to recognise right to privacy as a fundamental right.[19] Later on, there

[14] Centre for Law and Policy Research Trust. Constitution of India/ Debates, available at: https://www.constitutionofindia.net/debates/30-apr-1947/ (accessed: 19 May 2025)

[15] The United States Constitution, Fourth Amendment, available at: https://constitutioncenter.org/the-constitution/full-text (accessed: 19 May 2025)

[16] The Constitution of India, 1950. Gazette of India Extra. No. CA/83/ Cons./49. 26th Nov. 1949.

[17] *M P Sharma* v. *Satish Chandra, District Magistrate, Delhi* [(1954) SCR 1077)].

[18] *Kharak Singh* v. *State of Uttar Pradesh*, (1964) 1 SCR 332.

[19] See the observation of the Supreme Court in the *Justice K S Puttaswamy (Retd.), And Anr.* v. *Union of India and Ors.* (2017) 10 SCC 1, p. 352, para 15.

were other judgments by Apex Court declaring there is a right to privacy by highlighting various facets of right to privacy such as wiretapping, narco-analysis, gender based identity, medical information, informational autonomy and other manifestations of privacy.[20]

Finally in 2017, in *Puttaswamy* case[21], nine judges of Constitutional Bench unanimously have decided and settled legal issues revolving around right to privacy, especially the informational privacy. The facts of the case are simple. In 2009, the Indian government introduced one scheme known as *Aadhaar* scheme, that provided a unique 12-digit identification number to every resident of India. It was projected to enable easier access to government services and welfare programs. The *Aadhar* scheme required individuals to provide their biometric data, including fingerprints and iris scan for enrolment. This data was then stored in a centralizes database. The storage and accessibility of a vast amount of biometric data raised concerns about the government's potential for mass surveillance. In 2012, Justice K.S. Puttaswamy, a retired judge, has filed a Public Interest Litigation (PIL) in the Supreme Court of India challenging the constitutionality of the *Aadhaar* scheme arguing that it violates right to privacy due to the mandatory collection of biometric data without adequate safeguards and the potential for surveillance.

The judgment finally has declared that right to privacy is a right on which other rights, as recognised under the Constitution, derive their sustenance. The Court has declared that right to privacy is natural, primordial, basic, inherent and inalienable right. It is the base of liberty and dignity and directly related to it for meaningful exercise of liberties. Mere absence of express provision cannot be the reason to deny such right. Right to privacy is omnipresent and natural right of the individuals as well as group of individuals. The Court has highlighted three important components[22] of right to privacy—spatial control, decisional autonomy and informational control. It was held that the content of right to privacy can be positive as well as negative depending on the facts and circumstances of the case at hand.[23] It was held that right to privacy belongs to physical as well as mental aspects of life. Concerns of cognitive freedoms are dependent on privacy. It was highlighted that dignity and liberty at individual level are inextricably linked and privacy is a subset

[20] Ibid. pp. 400–401, para 102.

[21] Ibid.10 SCC 1.

[22] Ibid. p. 509, para 325.

[23] Ibid. p. 509, para 326.

of liberties. The right to privacy was held to be the inarticulate major premise of the Part III of the Constitution of India and not merely a derivative right.

Among the various facets of privacy discussed in the judgment, informational privacy received prominent attention. The Court, through six concurring judgments, has elaborated on the concept of informational privacy. It said that the interconnectedness of devices and computer sources create large amount of data. These data if seen in silos, may not make sense, but it becomes capable identifying the individuals, if the same is aggregated and then analysed.[24] Further, these data are capable of drawing inferences about personal characteristics and attributes of individuals.

As the Court pointed out, today the usage of Internet has made it difficult to ensure informational privacy. It has observed informational privacy relates to the person's right to determine when, how and to what extent information about him or her is to be communicated to others. It is a right to control personal information. Information which can lead to identification of individual if the same is accessed, used or disclosed. Supreme Court has highlighted: informational privacy requires that if personal information is provided by an individual to a third party, such parting of the information carries with it a reasonable expectation that the same will be utilised only for the specified purposes. The Court however, recognised the exception of legitimate interests of the State.[25] The Court has pointed out that prevention and investigation of crime, protection of revenue and good governance are some of the legitimate State interest for collection of personal information.[26]

The Supreme Court was of the view that the Parliament should enact laws to protect informational privacy. Such law should create a balance between the legitimate use of data by the State as well as non-state actors. The position of the Court was that any such law has to comply with three-fold requirements. Firstly, there has to be express legislation for curtailment of right to privacy, which must be substantive as well as procedurally fair law. Secondly, the law, even if it is for legitimate purpose, must be based on reasonableness as expected under Article 14 of the Constitution, and thirdly, the law has to be proportional. Curtailment

[24] Ibid. p. 500, para 300.

[25] Ibid. p. 501, para 301.

[26] Ibid. p. 505, para 312.

of right to privacy must be only when necessary and only to the extent which is necessary.

The observations of Supreme Court in *Puttaswamy* case about informational privacy in the times of internet and technology provides succinct insights on the need to have a robust legal framework for data protection.

2. Laying the Legislative Foundation: IT Act, 2000

Twenty-five years ago, in 2000, the Indian Government has enacted The Information Technology Act, 2000 (IT Act, 2000),[27] mainly to recognize electronic transactions and facilitates electronic commerce and address cybercrimes. This Act along with IT Rules[28] and Amendments[29] laid down foundational principles for informational privacy. Until the recent enactment of DPDP Act of 2023[30], the IT Act of 2000 was the primary legal framework for data protection and informational privacy. Though new specific law has been enacted in 2023, the provisions of IT Act 2000 still remain relevant for understanding the evolution of informational privacy law in India.

Before the enactment of IT Act the legal status of electronic data was ambiguous. Though the main objective of IT Act, 2000 was to provide legal recognition to electronic records and transactions, it inherently had privacy implications. By bringing digital data under the legal framework, the Act allowed the possibility of regulating the handling of digital data, thus protecting individual information.

One of the most important provisions in the IT Act 2000, relating to informational privacy is 43A[31], was added to the Act through an amend-

[27] Act No. 21 of 2000.

[28] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

[29] Particularly Information Technology (Amendment) Act, 2008.

[30] Act No. 22 of 2023. The DPDP Act hasn't yet come into force as it needs supporting Rules and Regulations, which are currently being developed by the Ministry of Electronics and Information Technology. These rules are crucial for outlining the operational framework and specifics of how the DPDP Act will be implemented and enforced. While the Act itself was passed and notified, the details needed to make it fully operational are still being finalized. The Ministry of Electronics and Information Technology (MeitY) has recently released draft rules are currently open for public feedback. he Act is likely to come into force in a phased manner, with specific provisions being notified by the government as the rules are finalized.

[31] Section 43A of the IT Act 2000 will be repealed once the Digital Personal Data Protection Act (DPDP Act) comes into force. See section 44 (2) (a) DPDP Act.

ment in 2008. It states that if a "body corporate" (any company, firm, sole proprietorship, or association of individuals engaged in commercial or professional activities) possessing, dealing with, or handling "sensitive personal data or information" in a computer resource is negligent in implementing and maintaining "reasonable security practices and procedures," and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the affected person. The IT Rules 2011, notified under section 43 A, explained "Sensitive Personal Data or Information" (SPDI)[32] includes passwords, financial information (bank account, credit/debit card, other payment instrument details), physical, physiological and mental health conditions, sexual orientation, medical records and history biometric information and any other information received by a body corporate for processing, stored, or processed under a lawful contract or otherwise, which falls under the above categories. It means that the information freely available in public domain or under the Right to Information Act, 2005 cannot be considered as SPDI.

Further, the IT Rules, 2011, also have defined what constitutes "reasonable security practices and procedures" to mean those security practices and procedures that are designed to protect information from unauthorized access, damage, use, modification, disclosure, or impairment. It also specified that compliance with the international standard[33] would be considered compliance with reasonable security practices.

The IT Rules, 2011 provided more specific details regarding data protection obligations. These Rules mandated several key practices for body corporates handling personal information and SPDI. It required body corporates to publish clear and easily accessible Privacy Policy on their websites.[34] This Private Policy must include the type of information col-

[32] The DPDP Act, 2023 on its enforcement, will omit Section 43A and the Sensitive Personal Data or Information Rules (SPDI Rules) under Section 43 A of IT Act 2000. See section 44 (2) (a) DPDP Act.

[33] IS/ISO/IEC 27001 (Information Technology–Security Techniques–Information Security Management System — Requirements).

[34] The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, Published by Ministry of Communications and Information Technology, G.S.R. 313(E), April 11, 2011, available at: https://www.indiacode.nic.in/handle/123456789/1362/simple-search?query=The%20Information%20Technology%20(Reasonable%20Security%20Practices%20and%20Procedures%20and%20Sensitive%20Personal%20Data%20or%20Information)%20Rules,%202011.&searchradio=rules (accessed: 19 May 2025). See Rule 4.

lected, the purpose of collection, who the information will be disclosed to, and the security practices employed. While laying emphasis on the consent of the Information Provider, the Rules required explicit consent for the collection and disclosure of SPDI.[35] The information provider must be given the option to opt out of providing such information and to withdraw their consent at any time.[36] It states the collection of data should be minimized to the actual necessity for required purpose.[37]

Moreover, the personal information can only be collected and used for the specific purpose for which it was initially collected[38] and should not be retained for longer period than required.[39] Most significantly, the Rules mandates that for disclosure of SPDI to a third party, prior permission from the information provider is required unless it's necessary for compliance with a legal obligation or agreed upon in a contract.[40] The third party receiving the data is also prohibited from further disclosing it.[41] To deal effectively with the grievances, the Rules require that body corporates must appoint a Grievance Officer and the details of the Grievance Officer must be published on their website.[42] This officer is responsible for redressing grievances of information providers within a stipulated timeframe of one month.[43]

Information providers have been given the right to review the information provided and request corrections for inaccuracies, if any.[44] Section 72A of IT Act, 2000 is another significant provision that provides for punishment for disclosure of information in breach of lawful contracts. It stipulates that 'any person, including an intermediary, who, while providing services under a lawful contract, secures access to personal information about another person with the intention of causing wrongful loss or wrongful gain, or discloses such information without the consent of the person concerned or in breach of a lawful contract, can be punished with imprisonment for a term up to three years, a fine

[35] Ibid. Rule 5(7).

[36] Ibid.

[37] Ibid.Rule 5(1)(b).

[38] Ibid.Rule 5(5).

[39] Ibid.Rule 5(4).

[40] Ibid.Rule 6(1).

[41] Ibid.Rule 6(4).

[42] Ibid.Rule 5(9).

[43] Ibid.

[44] Ibid. Rule 5(6).

up to five lakh rupees, or both.' It must be said this provision directly aims at protecting informational privacy by taking unauthorised disclosure of personal information seriously and penalizing unauthorized sharing of data obtained under a contractual obligation.

Some other provisions of the IT Act, 2000, though not directly focused on informational privacy, have indirect implications by criminalizing various cybercrimes. For instance, Section 43 provides penalty for unauthorized access, computer damage, and data theft. This helps protect the integrity and confidentiality of data, which is fundamental to informational m privacy. Section 66 punishes various cybercrimes like hacking, identity theft, and cyber fraud, often involving the unauthorized access or misuse of personal information. Section 69 that gives authority to the government to intercept, monitor, and decrypt information raises privacy concerns, it is intended to address national security issues due to cyber threats. Recognizing the importance of vital data system, Section 70 deals with the protection of critical information infrastructure

Despite these progressive provisions, the IT Act, 2000, had several limitations in safeguarding informational privacy. It primarily focused on cybercrimes and electronic transactions and not on data protection or informational privacy. It was applicable only to 'body corporates' and 'sensitive personal data', leaving other entities and types of personal information less protected. Unlike in many other jurisdictions, it did not provide for independent data protection authority to oversee compliance and enforcement. Though it incorporated provisions on consent and review, it lacked to provide certain upcoming rights to the information provider like the right to erasure (right to be forgotten) or data portability.

Thus, the IT Act, 2000, served as the foundational legal framework proving grounding for addressing the issues of informational privacy in India. Through Section 43A and the IT Rules, 2011, it introduced important concepts such as "sensitive personal data," "reasonable security practices," and the requirement for consent and a privacy policy. Section 72A further strengthened privacy by penalizing unauthorized disclosure. However, rapidly evolving global data protection regime and the constraints of IT Act, led to a more comprehensive and dedicated law, the Digital Personal Data Protection Act, 2023. This new Act aims to address the shortcomings of the IT Act, 2000, by providing a more robust framework for individual data rights, stronger obligations for data fiduciaries, and a dedicated regulatory body. Nevertheless, the IT Act,

2000, played a crucial role in laying the groundwork for recognising and protecting the informational privacy in India.

3. A Comprehensive Legislative Framework: DPDP Act, 2023

The Digital Personal Data Protection Act, 2023[45] was enacted by the Parliament that recognize right to informational privacy, providing a legal mechanism for processing of digital personal data. It provides a comprehensive framework, well explained by lots of Illustrations[46] attached to various provisions of the Act. It provides for responsible data handling, empowers individuals with greater control over their data, and ensures accountability for Data Fiduciaries (hereinafter DFs). The DPDP Act, 2023 is intended to provide for rights of Data Principals (hereinafter DPs) over their personal data.[47] The preamble of the law provides that DPDP Act, 2023 is intended to provide a balancing of interest between the protection of personal data and recognizing of digital data processing for lawful purposes.[48] The competency to enact this legislation by the Parliament can be traced to the Residuary clauses of the Constitution. The Constitution does not contain the word 'data' anywhere in the text or the Seventh Schedule, therefore, the Parliament has exercised its residuary power while enacting this legislation as provided in Article 248 of the Constitution of India.[49]

---

[45] The Digital Personal Data Protection Act, 2023 (hereinafter as the DPDP Act, 2023). It received the assent of the President on 11th August, 2023. The law is yet to be enforced as the commencement date of the same is not yet notified.

[46] For instance DPDP Act, See Sections 5-8.

[47] The DPDP Act comprises of forty-four Sections and a schedule. These forty-four sections are divided in nine chapters. First chapter of the legislation (Ss. 1–3) deals with preliminary matters, such as short title, commencement and the definition of words and phrases as used throughout the legislation. Chapter two of the legislation (Ss. 4–10) deals with obligations of data fiduciaries. Chapter three (Ss. 11–15) deals with rights and duties of data principals. Chapter four titled as 'Special Provisions' contain two sections i.e. section 16 and 17. Chapter five (Ss.18–26) is concerned with matters connected to establishment of Data Protection Board of India. Chapter six (Ss-27 & 28) deals with powers and functions of the Board. Chapter seven (Ss. 29–34) deals with appellate jurisdiction. Chapter eight (Ss. 33 & 34) contains provisions relating to penalties and adjudication. The last chapter of the law (Ss. 35–44) deals with miscellaneous matters and the only schedule attached to the DPDP Act, 2023 contains a list where quantum of penalties has been specified against breach of various provisions under the DPDP Act, 2023.

[48] See the Preamble of the Act.

[49] The Constitution of India. Article 248. (1) Parliament has exclusive power to make any law with respect to any matter not enumerated in the Concurrent List

The following pages provide a detailed account as to how DPDP Act addresses informational privacy.

3.1. The Commencement of DPDP Act

The DPDP Act was passed by the Indian Parliament in 2023 and received the assent of the President of India on August 11, 2023. It was published in the Official Gazette on the same day, thereby becoming law. However, the DPDP Act has not come into force so far at the time of writing this article.

The provision on commencement of the Act provides that the law will come into force as per the notification by the central government and the central government may provide different dates of commencement for specific provisions.[50] This law is yet to be enforced as the commencement date of the same by the central government is not yet notified. For its effective, implementation Act needs supporting Rules which are being developed by the concerned Ministry.[51] The Rules are required to provide clarity on the processes for obtaining consent, rights of Data Principals, grievance redressal mechanisms, technical and organizational safeguards, etc. functions and powers of the Data Protection Board of India (DPBI) etc.

These rules are crucial for outlining the operational framework and specifics of how the DPDP Act will be implemented and enforced. The Ministry of Electronics and Information Technology (MeitY) has recently released Draft Rules,[52] and made them open for public feedback. The government is likely to adopt a phased implementation approach, giving Data Fiduciaries, especially small and medium entities, time to build the necessary compliance infrastructure.

3.2. Applicability and Scope of the Act

Section 3 of the Act provides the scope of applicability of the legislation. It is provided that the Act is applicable in all those cases where pro-

---

or State List. (2) Such power shall include the power of making any law imposing a tax not mentioned in either of those Lists. Read with Entry 97 of the Seventh Schedule.

[50] The DPDP Act. Section 1(2).

[51] Ministry of Electronics and Information Technology (MeitY).

[52] See the Draft the Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology Notification, G.S.R. 02(E). Jan. 03, 2025.

cessing of digital personal data takes place within the territory of India irrespective of the fact, whether such data was collected in digital form or non-digital form, once the data has been digitized.[53] The Act is applicable in those situations as well, where data is being processed outside the territory of India but the purpose of such processing relates to offering of goods or services in India to DPs located in India.[54]

The same provision also deals with non-applicability of the Act. It is provided that the Act will not apply in two situations. These are (i) when data is processed by an individual for any personal or domestic purpose; and (ii) Such personal data has been made publicly available by the DP herself [55] or the data was made available publicly by any other person who is under a legal obligation to make such data public.[56]

The Act however, does not define the meaning of 'personal' as well as 'domestic' purposes. Concerns have been raised that this may lead to problems.[57] For example, what if a person A sends a courier to person B with the help of a company C. on the one hand, use of data by A may be considered personal but the processing of data by C may not be covered within the exception as provided. Similarly, processing of data by an individual for research will be personal purpose or academic purpose poses a question of concern, what if the research is conducted under the grants received by a funding agency, and research carried out for academic degree purposes? How the distinction is to be drawn? Similar questions may arise about the domestic and non-domestic use.

The Draft Rules provides the application of the Act is exempted when data processing is necessary for research, archiving or statistical

[53] The DPDP Act. Section 3(a) (ii).

[54] Ibid. Section 3 (b).

[55] Ibid. Section 3(c). The clause appears to have used words which are rendered redundant.

[56] Interpretation of Section 3(c) may pose problems. Use of the word 'and' in between clauses (i) and (ii) may become bone of contention. The word 'and' is generally used as a conjunctive word and not disjunctive, which means that when 'and' is used, both the conditions must be fulfilled. Although, the word 'and' in the present case preceded by a semicolon, which is generally understood as ending the clause which denotes that a new and independent clause begins. Therefore, there is a possibility of argument that both the clauses should be read conjunctively. It is submitted that these two clauses do not appear to be related as such and there is no common denominator between these two clauses hence, they should be read disjunctively.

[57] Meghna Bal, "Data Wrapped in Red Tape" *The Indian Express*, April 11, 2025, available at: https://indianexpress.com/article/opinion/columns/europe-data-privacy-9934892/ (accessed: 19 May 2025)

purposes and the standards as provided in the Schedule 2 of the Rules are followed.[58] Further, even the Draft Rules published does not mention the word "domestic" anywhere and leaves it open. It is also interesting to note: when the parent legislation uses the term personal, then the meaning of the same may not be constrained with the help of the subordinate legislation. Hence, the personal use cannot be simply restricted to research, archiving and statistical purpose. It is expected that the Rules will take into consideration this aspect and provide meaning and context of personal and domestic use.

3.3. Rights and Duties of Data Principals

The individual to whom the personal data[59] relates to, is called under the Act as Data Principal (DP) including child as well as any person with disability[60]. The Act recognizes various rights and duties of the DPs. One of the interesting things to be noted in the drafting of DPDP Act is that it uses the expression 'she' or 'her' to refer to all individuals as against the use of 'he', 'his' or 'him'. This is a welcome step to remove the linguistic bias that hitherto has dominated the legal language. The information providers under the DPDP Act have been called as Data Principal, which is departure from the GDPR nomenclature where they are called data 'subject'.[61] This may be a symbolic step but a better jurisprudential approach towards addressing the individuals as principals than the subjects of data concerning them.

---

[58] See the Draft Rules, Ministry of Electronics and Information Technology Notification, G.S.R. 02(E), Rule 15.

[59] The phrase 'personal data' has been defined to mean data about an individual who is identifiable by or in relation to such data. Thus, any data which contains the attribute(s) with the help of which an individual can be identified then such data becomes personal data. See Section 2 (t). The word 'data' has been used to mean information, facts, concepts, opinions or instructions if they are represented in a manner suitable for communication, interpretation, or processing by human beings or by automated means. See Section 2 (h). The word individual is used in the sense of natural person or human being. See Section 2 (s).

[60] The DPDP Act. Section 2 (j).

[61] See generally, Official Journal of the European Union, Regulation (Eu) 2016/679 of The European Parliament and of the Council, of April 27, 2016 "The Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed: 19 May 2025)

The first and the foremost right given to DPs is the right to obtain access to information about personal data available with the DFs. It is provided that when the DPDP Act comes into force, all the DFs are required to provide a summary to DPs about personal data which is already being processed. The DPDP Act also entitles the DPs to know about the identities of all other DFs and data processors who are processing such data. Also, DPs are entitled to information about the description of data which is being processed by such entities. In addition, the government may also prescribe by the Rules that what other information related to personal data of is required to be disclosed by the DFs.[62]

The next right—correction, completion and updating-- is dependent on the first right. If the DPs realize, after obtaining the information of the data available with the DFs, that there is error in data which is being processed by the DFs or on behalf of the DFs then DPs may get the same corrected, completed and updated.[63] This right of the DPs extend up to erasure of such data.[64] Exercise of such right of correction, completion, update and erasure has to be through a request made by DPs in the prescribed manner as provided by the DFs. However, in the legitimate State interest, despite the request for erasure being made, the data may be required to be retained for other specified purposes as may be prescribed under other legal obligation of the DFs under any other law.[65]

Another important right of the DPs relates to right to nominate any other individual in the event of death or incapacity of the DPs who can exercise the rights of the DPs in such eventualities.[66] The right to grievance redressal is also recognized as one of the important rights of the DPs.[67] It is provided that the DPs have right to grievance redressal by readily available means as provided by the DFs or data processors. This imposes a corollary obligation on the DFs and data processors to provide for access to such mechanisms which can provide opportunity of grievance redressal. The grievance redressal has to be within the specified timeline for which the rules is to be prescribed by the Central Government.[68]

---

[62] The DPDP Act. Section 11 (1) (c).

[63] Ibid. Section 12 (1).

[64] Ibid.

[65] Ibid. Section 12 (3).

[66] Ibid. Section 14.

[67] Ibid. Section 13.

[68] Ibid. Section 40(2)(o) .

The DPDP Act also provides for some of the duties that DPs are required to observe while exercising their rights. Though, the exercise of the rights is not dependent on performance of duties, however, it is a laudable provision where the DPs are expected to contribute in the better implementation of the Act. These duties include compliance with the provisions of the Act and all other relevant laws while exercising the rights under the DPDP Act. There is a duty not to impersonate another person while providing the details of another person for specified purposes, duty to ensure that there is no suppression of material information while providing personal data etc., there is a duty to not register false or frivolous grievance under the Act and duty to furnish only verifiable authentic information while exercising right to correction, update or erasure of data under the Act. The DPDP Act also empowers the Board to issue warning or impose cost in case of false or frivolous complaint being made by the DPs.[69]

3.4. Obligations of Data Fiduciaries and Data Processors

As stated above, the preamble of the Act recognizes lawful processing[70] of digital personal data[71] as one of the primary objectives of the legislation. The person[72] who determines the purpose and means of processing of data is called Data Fiduciary (hereinafter as DFs).[73] For the purpose of the Act, the DFs have been divided in two classes—Data Fiduciaries and Significant Data Fiduciaries (hereinafter as SDFs).[74] This SDFs is a special class of data fiduciary within the generic class. The Central Government is required to notify the persons who shall be considered as the SDFs on the basis of various factors such as volume

[69] Ibid. Section 28(12).

[70] Processing in relation to personal data, 'means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction' .See section 2 (x).

[71] The phrase 'digital personal data' is defined to mean personal data which is in digital form. See Section 2 (n) Even when personal data collected in non-digital form, but later on it was digitized, the Act becomes applicable to such data.

[72] Ibid. Section 2 (s) defines the word person in inclusive manner to include long list of juridical entities whether incorporated or not.

[73] Ibid. Section 2(i) .

[74] Ibid. Section 2(z) .

of data being processed by them, the risks to rights of Data Principals, impact on sovereignty and integrity, security of the State, public order and risk on electoral democracy.[75]

Apart from the DFs, another person who may be processing data is termed as Data Processor, they process data on behalf of DFs.[76] Other relevant concepts such as legitimate use,[77] specified purpose,[78] State[79] have been discussed later at appropriate stages. Obligations of the DFs can be understood as the core or the fulcrum of entire legislation. The first and the foremost obligation of the DFs relates to the compliance with the DPDP Act and other by-laws under the Act as a general-obligations.[80] It is provided that DFs shall process data only in accordance with the provisions of the Act and for lawful purpose only.[81] Lawful purpose refers to any processing which is not expressly forbidden by law. Processing may also occur for certain legitimate purposes as well.[82] The scope of legitimate purposes is defined in the Act to include various things discussed later in this part.[83] The next general obligation of the DFs relates to ensuring that data is complete, accurate and consistent when such data is to be utilized for the purposes of decision making related to DPs or when the same is being disclosed to any other DFs.[84] This obligation should be read along with the corollary right of the DPs to update, correct and complete data being processed by the DFs.

One of the most important obligations of the DFs relates to implementing the appropriate technical and organizational measures to ensure effective observance of provisions and rules prescribed under the Act.[85] The DFs are required to ensure that data in their possession remains protected and all measures reasonably necessary for such protection by them or the data processors should be in place as per the mandate of the law. In the event of breach of such data, there is an obligation

[75] Ibid. Section 10 (1).

[76] Ibid. Section 2(k).

[77] Ibid. Section 2(d).

[78] Ibid. Section 2(za).

[79] Ibid. Section 2(zb).

[80] Ibid. Section 8(1).

[81] Ibid. Section 4(1).

[82] Ibid.Section 4(2).

[83] Ibid. Section 7.

[84] Ibid. Section 8(3).

[85] Ibid. Section 8 (4).

on the DFs to intimate the same to the Board.[86] Also, data cannot be kept with the DFs for indefinite period and the same is required to be erased once the time period as specified in law is met or the consent has been withdrawn by the DPs unless retention of data is mandated by the law.[87] DFs are required to ensure that if the data is with the data processor on behalf of them, then such data is erased by the data processor. The DFs are also required to appoint the DPO (only in case of SDFs) or any other person who will answer the queries relating to data to the DPs.[88] Also, they have to ensure that business contact information of data protection officer (only in case of SDFs) or a person who is able to answer the queries raised by DPs relating to processing of personal data is made available to DPs. Also, the DFs are required to establish effective grievance redressal mechanism for DPs.[89]

It is the duty of DFs to provide notice to DPs for obtaining consent for data processing.[90] Such notice needs to contain the purpose of obtaining the consent in relation to data processing by the DFs. The consent by the DPs must be free, specific, informed, unconditional and unambiguous.[91] The consent should be obtained by a clear and affirmative action which should signify agreement to the processing of personal data for specific purpose and consent will be limited to such specific purpose as necessary for processing. Also, only that much data will be processed by the DFs as is necessary for the specified purposes for which the consent is obtained.[92] The contents of such notice have to be either in English or any other language as specified in the Eighth Schedule of the Constitution of India. Further, contents of the notice must be clear and in plain language.[93] Also, the notice itself should contain contact details of DPO or any person authorized by DFs to respond to communications from DPs for queries, concerns and exercising rights under the Act by DPs.[94] The DPDP Act also envisages similar duty of obtaining consent of the DFs in the transitory period as well. It is provided that when the

[86] Ibid. Section 8 (6).

[87] Ibid. Section 8 (7).

[88] Ibid. Section 8 (10).

[89] Ibid. Section 8 (9).

[90] Ibid. Section 5 (1).

[91] Ibid. Section 6 (1).

[92] Ibid.

[93] Ibid. Sections 5(3) and 6 (3).

[94] Ibid. Section 6(3).

consent of DPs was obtained prior to the enforcement of the Act, then at the time of the commencement of the Act, as soon as reasonably practicable, the DF must obtain consent as described above.[95] The consent in case of personal data of child or a disabled person refers to the consent of parent of such child or lawful guardian of such persons.[96]

Furthermore, it is the duty of DFs to inform DPs about the manner in which they can exercise various rights as recognized under the Act qua DFs such as right to correction, update or removal of data, right to withdrawal of consent, right to grievance redressal of the DPs etc. Also, DFs are required to ensure that process of withdrawal of consent has to be as easy as the process of obtaining the consent by the DFs.[97] In addition, DFs are required to inform DPs about the manner in which they can complain to the Board in case their grievances are not redressed by the DFs.[98]

DFs are required to cease processing of data once DPs have withdrawn their consent from such processing. Once the consent is withdrawn, then processing of data should not occur, except for the legitimate uses as prescribed by law. It is to be noted that the burden of proving that the processing of data is legitimate lies on the DFs. Also, the fact that DPs have not performed their duties as expected by the Act may not absolve the DFs from performing their duties or obligations.[99]

In the case of data concerning children, the law makes it obligatory that data processing must not take place in a manner that is detrimental to well-being of the child. Such processing must not lead to behavioral monitoring or targeted advertising and the processing must be in a manner which is verifiably safe manner.[100] There is additional obligation imposed on SDFs. They are required to mandatorily appoint a Data Protection Officer[101] and Data Auditor.[102] Also, SDFs are required to undertake periodic impact assessment of data protection, periodic audit and other actions as may be prescribed by the Rules in this regard.[103]

---

[95] Ibid. Section 5(2).

[96] Ibid. Section 9(1).

[97] Ibid. Section 6(4).

[98] Ibid. Section 5(1) (iii) read with Section 13(3).

[99] Ibid. Section 8(1).

[100] Ibid. Section 9.

[101] Ibid. Section 8(9).

[102] Ibid. Section 10 (2) (b).

[103] See generally Ibid. Section 10.

3.5. Legitimate Processing of Data and Exemptions

Legitimate use of personal data has been recognized under the Act in addition to processing of data for which consent has been obtained by DFs. Legitimate use may be by the DFs itself or by the State or any of the State instrumentalities.[104] The provision on legitimate use contains various grounds. The first legitimate use which is recognized relates to processing of data that has been shared by the DPs for specific purpose to the DF; and the processing of data by the DF for any other purpose for which she has not indicated that consent is not given to the use of personal data. Where personal data was shared at an earlier occasion by DPs for obtaining some benefit or any grant from the State, then in such situation, processing of data by the State instrumentality for granting any such or other benefits is considered legitimate.[105] Also, when data held by the State was in non-digital form, processing of the same may also occur for digitization purposes. However, in both cases standards and procedure for data processing must be in accordance with the Rules prescribed for the same.[106]

Further, personal data can be processed by the State for the purposes of performing any function as prescribed under any law or in the interest of sovereignty or integrity of India or for security of the State. Similarly, when data processing is necessary for fulfilling any obligation under any law which mandates disclosure of any information to the State, then also the data processing will be covered by legitimate use. Such processing is also required to be in adherence with the Rules in this regard. Additionally, processing of data in compliance of decree, judgment or order of the court, tribunal or any other regulatory institution which relates to contractual or civil nature may also be processed. Similarly, processing of data for employment purposes or for safeguarding the employer from loss or liability is also considered as a legitimate use. Another set of use which relates to safety of life and mitigation or prevention of disaster by various measure of provisioning of relief in such situation is also considered as a legitimate use.[107]

In addition to legitimate use, there are certain situations where specific purpose of processing is exempted from compliance of the man-

[104] See generally Ibid. Section 7.

[105] Ibid. Section 7(b).

[106] Ibid.

[107] See generally Ibid. Section 7, various clauses.

date of the law in relation to the obligations of DFs and rights of DPs.[108] These situations are: processing of data for enforcement of legal right; processing of data by the court, tribunal or an quasi-judicial or regulatory institutions; processing of data in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law; processing for the purposes of corporate restructuring as approved by the tribunal or any other authority established by law; processing of data of financial defaulters; contractual processing of data, where the DPs are not located in India and data is being processed in India by the contract where any of the parties to the contract is not located in India.

3.6. Powers and Functions of Various Functionaries under the Act

Apart from DPs and DFs, there are other functionaries which have been conferred various obligations, functions and powers under the DPDP Act. These functionaries are Consent Manager, Data Protection Officer, Data Auditor, Data Processors, Data Protection Board of India, Appellate Tribunal and the Central Government. The obligations, powers and functions of these functionaries are discussed below.

Consent Manager. It refers to a person who is registered with the Board for the primary function of acting as a single point contact for DPs on behalf of the DFs.[109] The Consent Manager is required to enable the DPs in managing, reviewing and withdrawing of consent in the accessible, transparent and interoperable manner.[110] Thus, Consent Manager acts like a bridge between the DFs and DPs. They have been made accountable to DPs.[111] The qualifications to register as consent manager and other technical requirements for the same are to be prescribed by the Rules to be notified by the Central Government.[112] If any grievance is made by the DPs, then Consent Manager is required to respond to such grievance within time specified in this regard.

Data Protection Officer (DPO). That Officer to be appointed by SDF[113] is required to represent the SDFs and acts as point of contact for griev-

[108] See generally Ibid. Section 17, various clauses.

[109] Ibid. Section 2 (g).

[110] Ibid. Section 6 (7).

[111] Ibid. Section 6 (8).

[112] Ibid. Section 6(9).

[113] Ibid. Section 10.

ance redressal mechanisms under the Act.[114] The individual based in India alone can be appointed as DPO and it will be responsible to the Board of Directors of the DFs. The functions of DPOs are similar to functions of person appointed by DFs for representing them under the Act as prescribed under Section 6(3).

Data auditor. Data Auditor refers to a person appointed by SDFs. The primary function of data auditor relates to carrying out data audit and other assessments and taking measures for data protection by SDFs.[115]

Data processors. It processes data on behalf of DFs. They are required to act as per the instruction of DFs.[116] The relationship between the DFs and Data Processors are supposed to be contractual and such contract has to be a valid contract.[117] Though, the Act does not expressly mention that the contract has to be written one, but it is expected that the Central Government may prescribe for the same through the Rules in this regard.

Data Protection Board of India. It is the prominent regulatory institution under the Act.[118] The Central Government is required to establish the same by a notification. Board is a body corporate. The Board shall comprise of a chairperson and other members.[119] Number of members are to be specified by the Central Government. The qualifications of chairperson and the members are same. It is provided by the Act that they should be persons of integrity and standing. The relevant experience may be related to the field of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, ICT, digital economy, law, etc. which in the opinion of the CG, may be useful to the Board. However, there must be at least one member from the discipline of law.[120] Primary functions of the Board relate to ensuring the Act is implemented properly.

The Act envisages that all consent managers will be registered with the Board[121] and such registration shall be based on essential conditions as prescribed by Rules relating to technical and other requirements ap-

[114] Ibid. Section 8(9).

[115] Ibid. Section 10 (2) (b).

[116] Ibid. Section 2(k).

[117] Ibid. Section 8 (2).

[118] Ibid. Section 2(c).

[119] Ibid. Section 19.

[120] Ibid. Section 19(3).

[121] Ibid. Section 6(9).

plicable to Consent Managers. The Board is expected to act as a first reporting authority in cases of data breach.[122] It is an obligation of DFs to inform the Board about breach in the manner prescribed. Once the Board receives the intimation about breach, the Board may give directions for mitigation and other purposes to contain the breach. It may conduct inquiry as well, into the cause of such breach.

Further, the Board is required to conduct inquiry and impose penalties in case of non-adherence of other mandates of law as prescribed by the Act or rules. The Board may receive complaint from the DPs with regard to data breach or non-adherence of the mandate in respect of rights of DPs about grievance not being addressed by DFs or consent manager. The Central and State government may also make a reference to Board, also, any court may also refer the matter to the Board for inquiry in relation to data protection or data processing.

In case of data breach or non-fulfillment of any obligation by DFs, the Board is required to conduct inquiry and it may impose penalty in case it is found that the breach is a significant one. Thus, a discretion has been conferred on Board that it may decide not to impose penalty in all cases. The discretion by the Board will be exercised keeping in mind nature of data breach, or other violation of mandate of law, along with factors such as gravity, duration of breach, type or nature of personal data affected by such breach, whether breach is recurrent one or repetitive, the nature of gain, if any, or loss to the person whose data has been breached, nature of mitigative steps taken by the person at default, the promptitude of the, the proportionality of the monetary fine imposition, and impact of fine if the same is imposed on person at fault.[123] Also, the Board is empowered to issue warnings or impose cost in those cases where it appears that nature of complaint is false or frivolous one.[124]

The Board is required to adhere to the principles of natural justice in proceedings before it and the law mandates that the Board will function as a digital office and physical appearance of the parties is to be avoided.[125] For the purpose of carrying out the functions under the Act, Board has been conferred with powers of a civil court.[126] The Board should

[122] See generally: Ibid. Section 27 deals with functions of the Board.

[123] Ibid. Section 33.

[124] Ibid. Section 28 (12).

[125] Ibid.Section 28.

[126] Ibid.Section 28 (7).

make an attempt to dispose the disputes or other grievances with the help of mediation amongst the parties or it may also decide to dispose the matter if the DFs make voluntary undertaking in matters where the primary grievance relates to non-compliance with the provision of the Act or the rules specifying the time for the compliance by DFs.[127]

Appellate Tribunal. To hear appeals from orders of the board, Appellate Tribunal has been provided for. Specific timelines have been provided under the Act with respect to disposal of the cases in appeal by the Tribunal.[128]

The Central Government. The Central Government is conferred with various powers under the Act in addition to notifying the commencement of the Act. For instance, the establishment of Board and appointment of chairperson and members of the Board are to be done by the Central Government. The primary responsibility of the Central Government relates to enactment of various types of Rules making implementation of the Act effective.[129] In addition, it is also the deciding authority with respect to exemptions of the mandate as provided for processing of data of children by such DFs for specific age bracket, who have adopted verifiably safe measures.[130] And the Central Government is also empowered to notify specific class of DFs who will be considered SDFs for the purposes of the Act.[131]

The Government is empowered to notify the countries where the data transfer will be prohibited[132]. The exemption from operation of law may be provided by the Central Government to any DFs are State instrumentality necessary for protection of the sovereignty or integrity of the nation, security of the state, friendly relations with any foreign state etc.[133]

In addition, the Central Government may also exempt the operation of law for research, archival or statistical purposes.[134] The Central Government is also empowered to provide exemption to startups.[135] Tempo-

[127] Ibid. Section 31.

[128] Ibid. See generally Sections 29-32.

[129] Ibid. Section 40.

[130] Ibid. Section 9 (5).

[131] Ibid. Section 10.

[132] Ibid. Section 14.

[133] Ibid. Section 17.

[134] Ibid. Section 17 (2) (b).

[135] Ibid. Section 17 (3).

rary exemption can also be notified by the Central Government when the notification for the same is notified in the initial five years from the date of the commencement of the Act.[136]

Apart from above powers, the Central Government's power with respect to blocking of the access of data by intermediaries is a powerful tool which is to be utilized cautiously and only when the conditions for the same are satisfied.[137] These conditions of blocking can be considered as triple test. Firstly, the Central Government should receive a reference from the Board intimating that a particular DFs has been imposed with a fine twice and secondly, the board advices that it is in the interest of general public that specific type of data should be blocked on the basis of which DF is able to offer the goods or services in India to DPs. Thirdly, the Central Government is also satisfied that such blocking is necessary for general interest of public. However, such blocking by the Central Government will be only after giving an opportunity of being heard to DFs.

4. Informational Privacy and Artificial Intelligence Algorithms

The DPDP Act is a remarkable piece of legislation protecting informational privacy. It is intended to provide a robust legal framework for processing of digital personal data while attempting to balance the rights of the Data Principals, and the need for data processing for the growth of business and other legitimate purposes. It is gratifying to note the Act, meets the international standards[138] and in certain cases is an improvement over those standards. The Act expressly contains data minimization principle and lawfulness principle with respect to processing of data.[139] Also, the Act provides that data processing is possible only with the consent, and for other reasons such as legitimate State interest, le-

[136] Ibid. Section 17 (5).

[137] Ibid. Section 37.

[138] See generally"India's Digital Personal Data Protection Act vs. the GDPR: A Comparison", available at: https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf (accessed: 19 May 2025). This report provides a tabular analysis of each and every provision of the DPDP Act, 2023 with GDPR and points out the parameters where the DPDP Act, 2023 matches with the GDPR. Also, it points out the cases where it has gone beyond GDPR and what provisions are lacking in comparison to GDPR.

[139] DPDP Act. See Section 4(1).

gal obligations and contractual necessity. These principles are generally considered as essential components of law dealing with personal data.

However, the Act makes no express mention of data processing by AI algorithms, though it seems to be within the ambit of the Act, as the definition of 'processing' refers to 'automated' processing as well. Further, concerns such as data bias and biased decision making due to algorithms do not find place in the legislation. However, the Act is not expected to operate in vacuum or isolation. The Indian legal framework specifically provides rights relating to equality, non-discrimination, respecting liberties of individuals which can be curtailed on specific grounds as prescribed by the Constitution of India and that too within the reasonable and proportionate measures of restrictions. Thus, the Constitutional regime mandates that decisions about a person by the State or any of its instrumentality cannot be arbitrary as the same goes against the principles of equality as envisaged under the Constitution of India.[140] Further, any decision which adversely affects an individual must be taken only after giving a reasonable opportunity of being heard and by respecting other principles of natural justice. Thus, if any decision, adversely affecting a person, is being made solely on the basis of AI, the same can be challenged on the ground of arbitrariness which violates the principles of equality and natural justice.[141] However, the mandate of natural justice, reasonableness, non-arbitrary decisions are applicable to State or State instrumentalities only. These principles are not binding, per se, on private persons as the fundamental rights are enforceable against the State only. Thus, to uphold fairness and accountability, DPDP Act should require that data-driven decisions of material consequence involve substantive human evaluation beyond algorithmic inference.

Further, the line between personal and non-personal, anonymized and non-anonymized data is subtle and blurred the era of AI. Thus, the DPDP Act is required to ensure that anonymization of personal data must be robust. The law needs to ensure that data cannot lead to identification of individuals or classes of individual even by a combination of anonymized data when the same is not expected. However, such provisions do not appear in the DPDP Act in its current form. The power of the Central Government in relation to Rule making may be utilized for such Rules which can prescribe such robust framework of anonymization of data.

---

[140] See generally the case of *Maneka Gandhi* v. *Union of India*, 1978 AIR 597.

[141] See R. Pal and P. Samaraditya. *MP Jain Indian Constitutional Law*. Chapter XXI.

Further, threats relating to the use of personal data of individuals, especially in the area of medical, health and life insurance surely pose challenges. Such data may provide real time analysis to insurance companies about health and lifestyle condition of individuals and may be highly determinative factor in deciding to offer of insurance and premium of the same. Therefore, law should provide for regulation of such data being used by companies. Thus, the law should contain provisions that ensure that the adverse decision making on the basis of data is supplemented by human intervention and is not based merely on the processed data. Provision may also be made that minimal data processing through AI should occur for legitimate State interest, contractual necessity. The legal obligation principle should be made a condition precedent for processing of the personal data through AI algorithms.

Conclusion and Suggestions

Since 2017, right to informational privacy is available, in India, against the State as a fundamental right and against non-state actors as a legal and common law right. The biggest challenge with respect to informational privacy arises from usage of internet, mobile technology and Internet of Things which have led to accumulation of large amount of data. Data about an individual or group of individuals can be used for various purposes and the same may prove beneficial as well as harmful to the individual and the society. The legal framework under IT Act 2000, has allowed and promoted the digital growth and various types of businesses have flourished in India in the last two and half decades. However, concerns of digital and cyber frauds etc. have rapidly escalated in the last decade, due to data leakage and data breach.

In 2023, the Indian Parliament enacted the standalone and dedicated law relating to informational privacy known as Digital Private Data Protection Act (DPDP Act). The DPDP Act may be regarded as a legislative framework that aligns with international standards for data protection and, in several aspects, even surpasses those global standards. A more in-depth analysis of the DPDP Act, however, reveals certain areas necessitating consideration for its improvement and enhancement.

Firstly, the DPDP Act, while encompassing automated data processing within its scope, does not explicitly address data processing by AI algorithms. Provisions to tackle some of the crucial issues like algorithmic bias and the resulting discriminatory decisions are absent from the DPDP Act. Though, the Act functions within India's broader consti-

tutional framework, which upholds equality, non-discrimination, and individual liberties and an adverse decision based solely on AI, can be challenged for violating constitutional guarantees, these constitutional safeguards primarily apply only to State actions and not to private entities. Hence, there is a pressing need for incorporating specific provisions in the DPDP Act mandating that consequential decisions derived from data analytics be subject to human oversight, rather than relying exclusively on algorithmic outputs.

Secondly, the line between the personal and non-personal, anonymized and non-anonymized data is becoming thinner and blurred in the era of AI. Hence, DPDP Act is required to ensure that anonymization of personal data must be robust and the same does not lead to identification of the individual or class of individuals even by a combination of anonymized data.

Thirdly, the classification of personal data and sensitive personal data, which has been dropped in the present Act finds relevance in this context. The Rules may prescribe that some sort of very personal data should be kept out of the purview of the processing by AI.

Fourthly, the DPDP Act not only fails to provide for the compensation to the victim of data breach, it also repeals Section 43A of the IT Act, 2000 that prescribed compensation to the victim of data breach. Again, the Rules may contain suitable provisions for the compensation.

Fifthly, DPDP Act does not prescribe maximum time limit for data retention by the State and this requires reconsideration by the legislature.

Lastly, the DPDP Act should certainly provide for educating the masses on informational privacy and the same should be made one of the primary functions of the Data Protection Board. The functions of the Board may also include carrying out and funding research in the area of informational privacy.

Addressing the abovementioned areas, through Rule Making or amendments, will surely strengthen the evolving right to informational privacy in India.

References

1. Al-Khassawneh Y.A. (2023) A Review of Artificial Intelligence in Security and Privacy: Research Advances, Applications, Opportunities, and Challenges. *Indonesian Journal of Science and Technology,* vol. 8, no. 1, pp. 79–96.

2. Artzt M., Tran V.D. (2022) Artificial Intelligence and Data Protection: How to Reconcile both Areas from the European Law Perspective. *Vietnamese Journal of Legal Sciences,* vol. 7, no. 2, pp. 39–58.

3. Bakshi P. M. (2025) *The Constitution of India*. Delhi: Universal Law Publishing, 205 p.

4. Carey P. (2020) Data Protection: a Practical Guide to UK Law. Oxford: Oxford University Press, 689 p.

5. Dass R., Sharma A. et al. (2024) Artificial Intelligence in Media Marketing and Law. Delhi: Bloomsbury, 224 p.

6. Halder D., Jaishankar K. (2012) *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations.* Hershey: IGI Global, 267 p.

7. Jain A. K., Jain S. (2025) Lead Smart in the AI Era. Delhi: Rupa Publications, 280 p.

8. Kamath N. (2012) Law Relating to Computers, Internet and E-Commerce. Gurgaon: LexisNexis, 847 p.

9. Kranenbarg W., Leukfeldt R. (2021) Cybercrime in Context: the Human Factor in Victimization, Offending, and Policing. Cham: Springer, 407 p.

10. Kumar S. (2021) Textbook on Information Technology Laws. Delhi: Whitesmann Publishing Co., 464 p.

12. Lumsden K., Harmer E. (2019) *Online othering. Exploring Digital Violence and Discrimination on the Web.* Cham: Palgrave Macmilan, 407 p.

11. Kuner C. et al. (2018) Expanding the Artificial Intelligence-Data Protection Debate. *International Data Privacy Law,* vol. 8, no. 4, pp. 289–292.

14. Pal R., Samaraditya P. (2025) *MP Jain Indian Constitutional Law*. 6th ed. Delhi: Lexis Nexis, 499 p.

13. Nanda S. K. (2021) Media Law. Prayagraj: Central Law Publications, 497 p.

15. Radu R. (2019) *Negotiating Internet Governance*. Oxford: Oxford University Press, 228 p.

16. Rajput B. (2020) *Cyber Economic Crime in India: an Integrated Model for Prevention and Investigation.* Cham: Springer, 262 p.

17. Ryder R.D., Naren N. (2020) Internet Law. Delhi: Bloomsbury, 539 p.

18. Shah N. (2024) *AI and Social Ethics: Gandhian Approach.* Jaipur: Rawat Publications, 220 p.

19. Sharma V., Sharma S. (2023) *Information Technology Law and Practice: Cyber Laws and Laws Relating to E-Commerce, Privacy, Social Media, Defamation.* Delhi: LexisNexis, 694 p.

20. Viano E.C. (2017) *Cybercrime, Organized Crime, and Societal Responses: International Approaches.* Cham: Springer, 378 p.

21. Westin A.F. (1968) Privacy and Freedom. *Washington and Lee Law Review,* vol. 25, no. 1, p. 166.

23. Yanamala A.K., Srikanth S. (2023) Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Engineering Technologies and Innovations,* no. 1, pp. 294–319.

23. Završnik A., Simončič K. (eds.) (2023) Artificial Intelligence, Social Harms and human Rights. Cham: Palgrave Macmilan, 276 p.

Information about the authors:

U. Tandon — Senior Professor.

N.K. Gupta — Assistant Professor.

The article was submitted to editorial office 26.05.2025; approved after reviewing 12.06.2025; accepted for publication 12.06.2025.