RIGHT TO PRIVACY AND DATA PROTECTION ACT: AN ANALYTICAL STUDY

Nandini Sinha, Assistant Professor of Law at Apeejay Stya University, Haryana and PhD Research Scholar at Amity Law School, Amity University, Haryana

ABSTRACT

This research paper examines Data Protection and security of personal data in the context of Right to Privacy in India. The proliferation of data has increased greatly in the last few decades with the expansive use of internet and highly advanced technology. Huge amount of personal data of people are being accumulated, stored, processed and distributed by a number of entities, businesses and organizations. In this backdrop, it becomes even more significant to secure the privacy of individuals as the scope of data breach has become greater. The evolution of Data protection regime has been fascinating and Indian lawmakers have taken inspiration from the existing international framework to draft a comprehensive data privacy and protection law. The efforts of the lawmakers culminated into the enactment of "The Digital Personal Data Protection (DPDP) Act, 2023". The author has relied on a detailed literature review to highlight the Key aspects of the Act, identify the inherent issues in the Act and suggest reforms.

This paper analyses the efficacy of current measures and legislative framework in addressing the concerns of data breach and consequently, securing and protecting personal data.

This paper attempts to expend to the current jurisprudence on data protection. By highlighting the issues in the data protection regime, this paper aims to recommend suggestions, expand public awareness and assist in better enforcement of the Act.

Keywords: Data Protection, Privacy, Data Breach, Personal Data, Security

1.1 INTRODUCTION

The notion of Privacy has evolved considerably in the last few years. Every person has an innate desire to safeguard his privacy and dignity. To put it simply, privacy can be viewed from a multi-dimensional standpoint and holds different meanings, varying from culture to culture and region to region. In today's times, every individual seeks to safeguard his privacy owing to a substantial increase in technological developments and proliferation of social media. The world has increasingly become digital with growing domestic and cross border inter-connectedness amongst individuals, businesses, government and non-government entities etc. In this context, it becomes even more significant to protect one's privacy. There is huge amount of data pertaining to personal information, financial information etc, floating on the web. The lack of transparency in the manner in which this data is being collected, stored, accessed and processed is a matter of concern. There have been numerous instances of privacy violations wherein sensitive information of individuals such as credit card details, health information, bank account details, contact details etc. have been leaked. In this background, a need was felt to bring a comprehensive legislation to tackle such challenges. After a lot of deliberations and discussions, the legislature enacted the "Digital Personal Data Protection (DPDP) Act, 2023"[1], hereinafter referred to as DPDP Act. However, being a recent legislation, the efficacy of the DPDP Act needs to be analysed in the context of how well it protects the privacy of individuals by securing personal data and whether it fulfils its aim of appropriately striking a balance between "the need to process such personal data for lawful purposes" and "the right of individuals to protect their personal data," as stated in the Act's preamble.

1.2 REVIEW OF LITERATURE

An extensive review of literature was undertaken by the author including relevant books, journals, articles, essays, government websites, websites of international bodies, newspapers etc. some of which are mentioned below:

1.2.1 Books:

(i) Dr. JN Pandey in his book **"Constitutional Law of India",** [2] has elaborated on the

[1]THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[2] J.N. Pandey, Constitutional Law of India, Central Law Agency, 61st edition (2024)

evolution of Right to privacy tracing it in historical context with references to various cases including the Recent landmark cases.

(ii) MP Jain in his book **"Indian Constitutional Law"**[3] has also discussed about the Right to Privacy as a part of fundamental freedoms guaranteed by the law of the land. The important cases have also been highlighted.

(iii) Sanjay Jain in his book **"V.D. Mahajan's Constitutional Law of India"**[4] has thoroughly discussed about the various contours of privacy as a right and highlighted its development through the assistance of diverse case laws.

1.2.2 Research papers:

(i) Kumar NH in his paper **"A Study on Right To Privacy And Data Protection In The Cyber Space"**[5] highlighted the relevant aspects in the best protection of data alongwith privacy of the individuals in cyberspace and best use of the technology with focus on laws such as Information Technology Act, 2000.

(ii) Paulo Campanha Santana and **Faiz Ayat Ansari**, in their paper **"Data Protection And Privacy as a Fundamental right: A Comparative Study of Brazil And India"**[6] have drawn a comparative study between India and Brazil and analysed how both the countries faced the issue of a massive amount of personal information of people being exchanged, stored, processed etc. The authors have discussed the concepts of Data protection and privacy in detail and recognized that the rights to personal data and privacy were not unqualified and needed to be weighed against other societal interests.

(iii) **Payal Thaorey** in her paper, **"Informational Privacy: Legal Introspection in India"**[7] has discussed about the concept of privacy with emphasis on technology and informational privacy while focusing on relevant legislations.

[3] MP Jain, Indian Constitutional Law, Lexis Nexis, 9th edition (2024)
[4] Sanjay Jain, V.D. Mahajan's Constitutional Law of India, Eastern Book Company, 8th edition (2023)
[5] Kumar NH, "A Study on Right To Privacy And Data Protection In The Cyber Space",Vol.6,No.4, International Journal of Creative Research Thoughts (2018)
[6] Paulo Campanha Santana, Faiz Ayat Ansari, "Data Protection and Privacy as a Fundamental right: A Comparative Study Of Brazil And India", Vol.9, No.3, Journal of Liberty and International Affairs (2023)
[7] Payal Thaorey, "Informational Privacy: Legal Introspection In India", Vol. II, ILI Law Review (2019)

1.2.3 Other Sources:

(i) Reports: A number of commission and organization's reports pertaining to the research issue were also taken into consideration.

(ii) Newspapers: The literature on this subject was reviewed using a few national dailies, including The Hindu, The Indian Express, and Hindustan Times, among others.

(iii) Websites: To extract the most recent information, quite a few websites were examined, including SCC online, Meity, Manupatra, Research gate, Jstor etc.

1.3 STATEMENT OF PROBLEM

Over the last few years, the world has seen increasing digitization and consequently, large amount of data being collected, stored, processed and exchanged by and amongst various entities. There is a lack of transparency when it comes to safeguarding the personal data of individuals and there have been innumerable instances of personal information leak which ultimately violates the Right to Privacy of individuals. There is a need to analyse the problem in detail, identify the challenges pertaining to data protection including its implementation in the light of DPDP Act in particular and the Right to Privacy in general.

1.4 OBJECTIVE OF STUDY

1. To analyze the Concept of Privacy with reference to Data.
2. To analyze the present statutory framework governing data protection in India.
3. To examine the key aspects of the "DPDP Act, 2023".
4. To identify the limitations of the "DPDP Act, 2023".
5. To suggest recommendations for refining data protection regime.

1.5 RESEARCH QUESTIONS

1. What is meant by Privacy in the context of Data?

2. How efficient is the current statutory framework governing data protection in India?

3. What are the key aspects of the "DPDP Act, 2023"?

4. What are the limitations of the "DPDP Act, 2023"?

5. What are possible recommendations for refining data protection regime?

1.6 METHODOLOGY

This study analyses data protection and privacy law by way of doctrinal research and qualitative as well as quantitative techniques, primarily relying on secondary sources such as the constitution, various statutes, books, journal articles, research papers by multiple authors, reports of various commissions, organizations, media sources, newspapers which were the foundation for the analysis.

1.7 CONCEPT OF PRIVACY IN CONTEXT OF DATA

It is pertinent to understand the concept of Privacy and the meaning of the term 'data' in order to gauge data protection in the broader context of Right to Privacy. The origin of Privacy can be traced back to the term "Privatus" which essentially entails being separated from the rest of the world. Though the term Privacy has not been uniformly defined, it can simply mean absence of intrusion into one's personal space. It has also been defined as the right to be let alone. Privacy is intrinsically linked to individual autonomy and enables the development of an individual to their full potential. Privacy lies at the core of individual liberty, enabling people to make personal decisions without undue intrusion. It includes the ability to manage personal information, preserve confidentiality, and act independently without external interference. Privacy has been widely recognized as a component of human rights and has been duly acknowledged in many international conventions and treaties such as International Covenant on Civil and Political Rights- "*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation*[8]", European Convention on Human Right-"*Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and*

[8] International Covenant on Civil and Political Rights, art. 17(1)

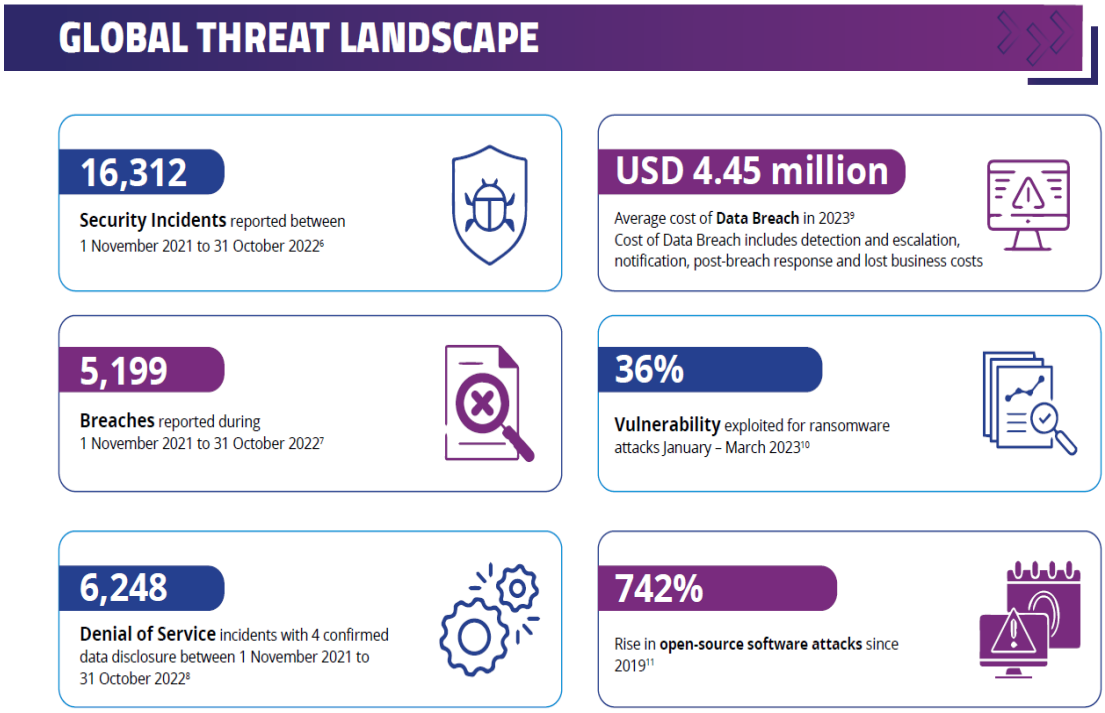
is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[9], Universal Declaration of Human Rights- "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*."[10]

The Right to Privacy also finds place in Indian Jurisprudence and has developed exponentially over the past few years. The Apex Court, in the celebrated **Puttaswamy** judgment[11] gave recognition to the Right to Privacy as a Fundamental right which is protected as a fundamental element of personal liberty and also the right to life under Article 21 and as an integral part of the freedoms assured by Part III of the Constitution. This landmark case gave an impetus to Privacy as a right and marked a significant step in the evolution of Constitutional history, especially as earlier Judgments such as **MP Sharma**[12] and **Kharak Singh**[13] stated that Right of Privacy cannot be said to be a guaranteed right under the Constitution of India. Privacy is essential for human dignity and other freedoms cannot be effectively and meaningfully enjoyed if Privacy is hindered. However, it is important to keep in mind that the fundamental right to Privacy is not absolute in nature and is liable to be subjected to certain reasonable restrictions if the need arises.

The term 'Data' entails measurements or observations which is collected as a source of information. They come in various forms and can be represented in multiple ways. For example, data pertaining to population of a country, literacy rate, unemployment statistics etc. According to European Union's GDPR[14], "Personal data can be referred to as something which helps in the identification of persons. Information that can directly or indirectly identify individuals such as their name, location, or unique traits reflecting their mental, physical, economic, physiological, cultural, or social identity is deemed identifiable." Essentially, this includes any data that is or could be associated with a person. For instance, a person's phone number, account information, credit card number, details related to one's height, weight, health, marital status, education are all examples of personal data. Data protection in the

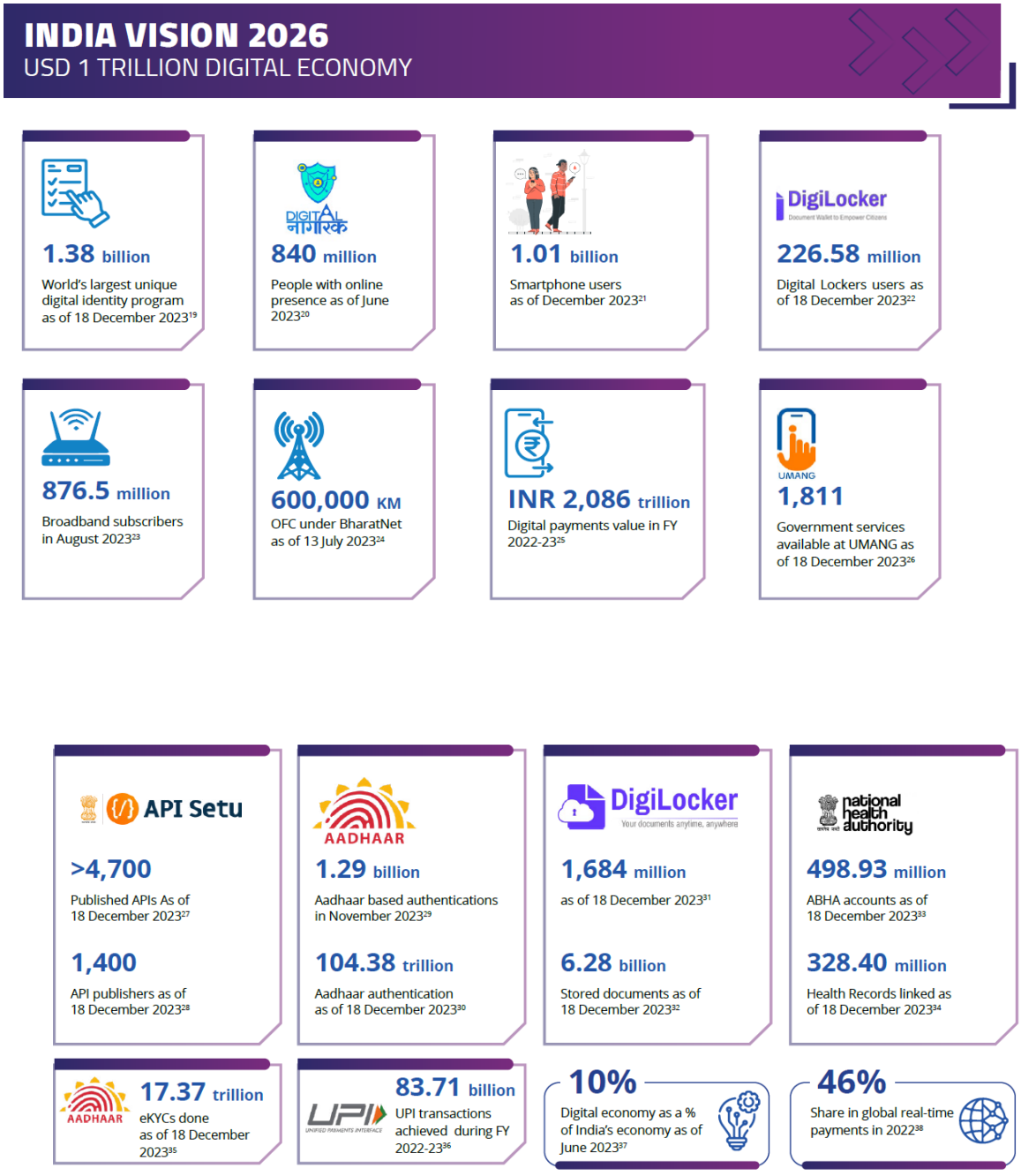
[9] European Human Rights Convention, art. 8
[10] Universal Declaration of Human Rights, art. 12
[11] Justice K.S. Puttaswamy and Anr. v. Union of India and Ors. (10 SCC 1, Supreme Court of India, 2017)
[12] MP Sharma v Satish Chandra, AIR 1954 SC 300
[13] Kharak Singh vs State of UP, AIR 1963 SC 1295
[14] General Data Protection Regulation. art. 4

context of Privacy is primarily concerned with the fact that individuals should have the means and autonomy to safeguard their data. Personal Data should not be subjected to unauthorized use, that is without the consent of the individuals. Data breach is becoming a common issue these days, especially with the advent of advanced technology which facilitates collecting, storing, processing and distribution of data instantly. There have been an alarming increase in data leak of people which is highlighted in a recent report[15] by Data Security Council of India (DSCI) below. Furthermore, the report also highlighted the increasing digital footprint of people and availing of digital services by people in large numbers, especially when the Government is aiming to fulfil "India's vision of becoming Digital economy of US Dollars 1 trillion".



Source: "India Cybersecurity Domestic Report 2023, DSCI"

[15] India Cybersecurity Domestic Report 2023, https://www.dsci.in/resource/content/india-cybersecurity-domestic-report-2023 (last visited on December 18, 2024)



Source: "India Cybersecurity Domestic Report 2023, DSCI"

In this context, it becomes imperative to have a secure data protection framework which enhances the privacy and safety of people. It is pertinent to note that most of the developed nations already have an elaborative data security and protection regime in place, which gives an added sense of safety to their people. While the challenges being faced by developing countries like India is understandable, it cannot be ignored that there is a pressing need to ensure the safety of data or personal information of people. It is to be noted that one cannot

truly exercise their liberty when there is a constant threat to their privacy. Privacy has already been afforded a status of fundamental right and has been provided recognition as a form of human rights closely interlinked with dignity and respect of people. In this day and age, privacy holds considerable significance as personal data of people is at a risk of being compromised and threatened not only by state agencies in the garb of surveillance but also by other private entities and institutions. There is a greater need than ever before to secure the protection of privacy of people and to strongly safeguard their personal information.

1.8 STATUTORY FRAMEWORK GOVERNING DATA PROTECTION IN INDIA

With the growing cases of data breach and lack of adequate laws, a need was felt to develop a comprehensive legislation to secure the personal data of people. It is not to say that there was no provision to tackle such issues earlier, in fact Data protection and privacy regulations in India trace their roots to the "Information Technology Act"[16] and the "IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011". These legal measures marked initial efforts to create a framework for safeguarding data and privacy.

(i) Relevant Provisions under "The Information Technology Act, 2000":

The Act defines data under Section 2 as "*data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer*."[17]

Furthermore, Section 43A provides for Compensation in case of failure to protect data–"*Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, 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*

[16] The Information Technology Act, 2000 (Act 21 of 2000)
[17] The Information Technology Act, 2000 (Act 21 of 2000), s. 2(1)(o)

compensation to the person so affected"[18].

Moreover, according to the Explanation to Section 43A, "reasonable security practices and procedures" refers to security measures intended to prevent unauthorized access, damage, use, modification, disclosure, or impairment of the information. These measures may be specified in an agreement between the parties or in any currently enacted law, or in the absence of such agreements or laws, "reasonable security practices and procedures" may be prescribed by the Central Government in consultation with any professional bodies or associations it deems appropriate. Additionally, "sensitive personal data" refers to any personal information that the Central Government may prescribe after consulting with the relevant professional bodies.

However there are certain provisions in the act which place limitations on privacy, one such provision is Section 69 which permits surveillance by the Central and State governments and gives government agencies authority to "intercept, monitor, or decrypt" data based on a variety of grounds, such as the defence of India, friendly relations with foreign states, public order, or in the interest of the sovereignty or integrity of India.[19]

(ii) The Digital Personal Data Protection (DPDP) Act, 2023:

The DPDP Act was passed by the Indian Parliament recently in August 2023. It is the first ever comprehensive law on the protection of Personal data of people, culminated after considerable deliberations and revisions of earlier bills dealing with the same subject. Instrumental among these was the Personal Data Protection Bill, 2019. The bill provided for setting up Data Protection Authority (DPA), a significant data protection regulator, which would oversee the proposed cross-sectoral data protection laws. The bill laid the groundwork for prevention. It mandated that companies that collect personal information take informed consent of individuals, keep accurate information safe, and use it only for the reasons stated in the notice. Additionally, businesses had to allow users to view, delete, and port their data, as well as to destroy it once its intended purpose was fulfilled. Furthermore, Companies had to establish grievance resolution procedures, enforce "privacy by design" regulations, and maintain security measures and transparency standards. Also, the bill provided for "consent managers," who were basically intermediaries responsible for collecting and giving consent to

[18] *Id.,* s.43A
[19] *Id.,* s.69

companies on behalf of persons.[20] Another significant feature of the bill is that, for a number of reasons, including lawful state functions, public order breakdowns, processing data related to employment, health and medical services during epidemics and emergencies, preventing and detecting unlawful activity, whistleblowing, etc. the 2019 bill exempted specific entities and businesses from notice and more importantly, consent requirements.

Justice B.N. Srikrishna, a former Supreme Court judge, served as the chair of the Srikrishna Committee, which was formed by the Ministry of Electronics and Information Technology in 2017 to define data protection standards. The committee's 2018 draft bill served as the primary basis for the regulatory structure of the 2019 bill.

However, 2019 bill suffered from certain inherent limitations, to rectify the same certain improvements were made, finally leading to the formulation of The Digital Personal Data Protection DPDP Act, 2023 which was based on 2022 draft. The DPDP Act adopted a significantly different approach from the 2019 bill and marked the introduction of India's first comprehensive data privacy law. The term data is defined in the act as- "*data means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means*"[21]. According to the act, consent is required for processing personal data, with specific exceptions which have been outlined in the legislation. The law grants individuals the rights to access, amend, update, and delete their data, along with the ability to nominate others to manage it. Moreover, special protections have been included for processing children's data. Businesses must adhere to purpose limitations, notify users about data collection and processing, and implement strong security measures. They are also required to establish grievance redress systems. The Data Protection Board (DPB) is tasked with resolving complaints, addressing grievances, and imposing penalties for violations.

There are many revolutionary aspects in the DPDP Act which aims to overhaul the way in which data is collected, processed, stored and handled. The act has been drafted with the view to protect and enhance security over personal data of people. The act itself and also the previous versions of the bill had been drafted after considerable thought and keeping in conformity with

[20] Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?," Carnegie India, https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217 (last visited on December 19, 2024)
[21] The Digital Personal Data Protection Act, 2023 (NO. 22 OF 2023), s. 2(h)

international data protection and privacy standards and protocols. In a nut shell, the act attempts to strengthen privacy and security in the digital realm, and is evidence of a remarkable shift in the approach for safeguarding online identities.

1.9 KEY ASPECTS OF THE DPDP ACT, 2023

DPDP Act, 2023 serves as an important piece of legislation dealing with data protection in the background of growing data breaches across the country. There are certain important aspects of the Act which are highlighted below:

(i) **Application of the act:** The Act governs the processing or refining of digital personal data within India, whether the data is originally collected in digital form or first collected in non-digital form (physical or offline mode) and later digitized. It also applies to the processing of digital personal data outside India if it is connected to activities such as offering goods or services to Data Principals in India.[22]

(ii) **Requirement of clear objective or purpose:** The Act clearly enumerates that personal data to is to be processed for any lawful purpose, either with the consent of individual or alternatively for "legitimate uses". The Consent shall be “free, specific, informed, unconditional, and unambiguous,”[23] and for the said purpose. The collection of data must be limited to the said purpose. Individuals must receive a clear notice explaining these terms, including their rights and the grievance redress process. Furthermore, individuals can also withdraw their consent.

"Legitimate uses" cover the following scenarios:

a) Furnishing of personal data by individuals for a specific or particular purpose. This should be voluntary.

b) Delivery of “subsidies, benefits, services, licenses, certificates, or permits by state entities”, if the person has earlier provided his consent to similar services.

[22] *Ibid.,* s.3
[23] *Id.,* s.6

c) Issues concerning sovereignty or national security.

d) Compliance with obligations of legal nature requiring disclosure to the state.

e) Adherence to judicial orders, decrees, or rulings.

f) Addressing "medical emergencies, epidemics, or public health concerns".

g) Dealing with disasters or restoring public order.[24]

(iii) **Rights of Individuals or data principals**:

The act provides for following rights of individuals: "Right to access information about personal data, correction and erasure of data, redressal of grievances and nomination right".[25]

(iv) **Duties of Data fiduciary:** Under the Act, establishments which are responsible for collection, storing, and refining of digital personal data, are known as "data fiduciaries", they are required to perform specific duties or obligations, which are enumerated below:

a) Implement robust security measures to safeguard personal data.

b) Ensure the accuracy, completeness, and consistency of the data.

c) Report data breaches to the "Data Protection Board of India (DPB)" as per prescribed guidelines.

d) Delete data when consent is withdrawn or the specific purpose is achieved.

e) Appoint a data protection officer and implement mechanisms for redressing of grievance.

f) Obtain parental or guardian consent for processing data related to children or minors.

[24] *Id.,* s.7
[25] *Id.,* ss. 11;12;13;14

The Act also prohibits activities that may harm children, such as tracking, behavioral monitoring, and targeted advertising. However, the government may prescribe exemptions to these provisions for certain purposes.[26]

1.10 LIMITATIONS OF "THE DPDP ACT, 2023"

The Act, though a game changer in the area of data security and privacy lacks in certain aspects. The limitations pertaining to the Act are briefly discussed below:

(i) Some organizations and purposes are entirely exempted from the Act's application. These include processing in support of India's integrity and sovereignty, state security, amicable relation with other nations, upholding public order, or avoiding incitement to any offence. This will enable security and investigative organizations to continue operating outside the scope of this act.

(ii) Data processing required for "archival, statistical, or research", purposes if the personal information isn't going to be a deciding factor which are specific to a data principal.

(iii) The consistency, correctness, completeness, deletion and notice provisions may be waived off by the government for particular groups of data fiduciaries, which may include startups.

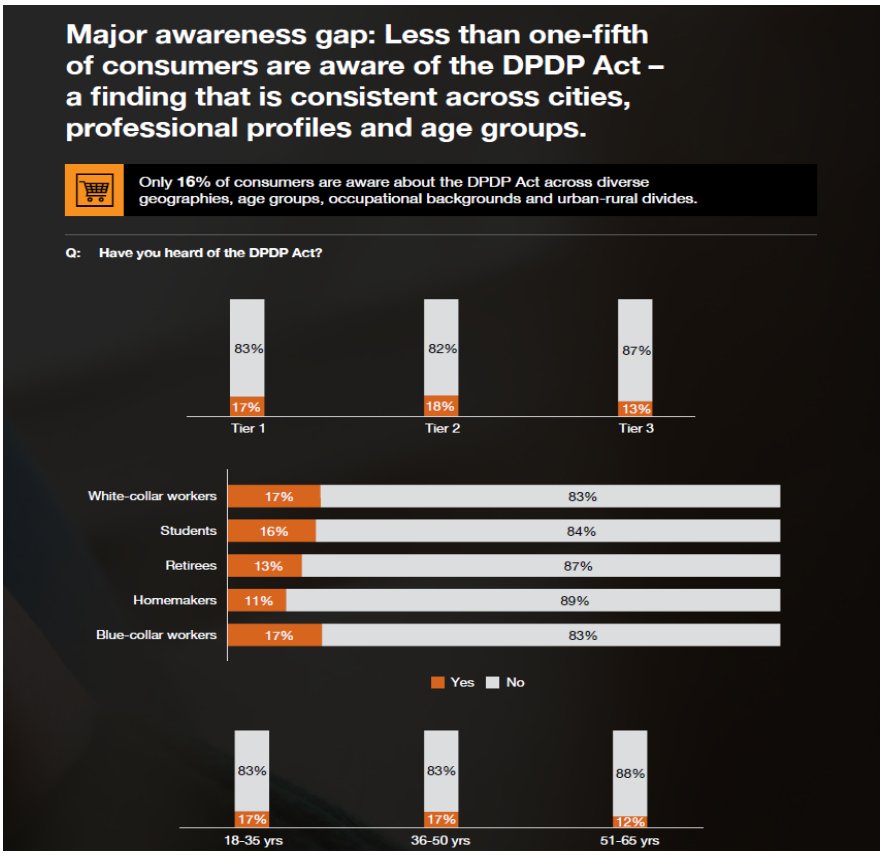
(iv) Another questionable provision permits the government to declare that particular "data fiduciaries or classes of data fiduciaries" will not be subject to any of the Act's provisions for a time that may be specified in the notice, "before expiry of five years from the date of commencement of this Act".[27] There is a lack of specific rules governing the reasons for exemption, the kinds of persons who may be excluded, and the time period during which such exemptions will last, thus it will not be incorrect to infer that this is a wide and significant discretionary power.

(v) By virtue of another provision i.e. ***Section 7(b)*** the concerned government can avert consent requirements where an individual (i.e. beneficiary) of government services

[26] *Id.,* ss. 8;9
[27] *Id.,* s.17

has earlier consented to accept any other benefit or advantage from the state. In addition to making it easier to get beneficiaries personal information for the objective of delivering government services, this enables the government to create databases. This is because government entities would have to be excluded from purpose restrictions, which necessitates that personal data be erased after its intended use has been completed, in order to fully implement this law.

(vi) Apart from the above, another challenge is going to be in the implementation of this act meaningfully at the ground level as there is still considerable lack of awareness about this act among the masses. This is evidenced from a recent survey[28] conducted by PWC in 2024 which has highlighted lack of awareness among consumers. Important data from the study is highlighted below:



Source: PWC Survey, 2024

[28] How aware and prepared are Indian consumers and businesses to navigate the new era of digital privacy? A survey of India's data privacy landscape. https://www.pwc.in/assets/pdfs/aware-prepared-indian-consumers-businesses-navigate-new-era-digital-privacy.pdf (last visited on December 19, 2024)

Source: PWC Survey, 2024

The aforementioned PWC survey also concluded the following:

a) Awareness about privacy and data security in India is at below par level. But still it is somewhat a positive beginning as our country has a huge and diverse population which varies considerably in terms of education, literacy levels etc.

b) Certain entities such as sectors which are regulated and d2C (direct to consumer) sectors are more aware and foster an environment of data security, however they do reflect concerns about the act, the manner of its enforcement and its consequences.

c) There is a lack of trust among individuals on the way in which companies gather and store their information.

d) A strong requirement for a cultural shift is the need of the hour as it will give an impetus to data security and protection.

1.11 RECOMMENDATIONS FOR REFINING DATA PROTECTION REGIME

The present DPDP Act, though a well-crafted legislation with a good intent, suffers from certain limitations as discussed above. In light of the same, following recommendations may be taken into consideration for refining data protection:

(i) The earlier version of the Act that is the 2019 Bill had provided for "Data Protection Authority" (DPA) which had more effective powers compared to the present "Data Protection Board" (DPB) under the DPDP Act. DPB has a limited role mainly being confined to penalty impositions and issuance of directions in the event of non-compliance. Further, it has insufficient power to make regulations, focusing more on taking rectifying action in the instances of breach of data. There is a need to review the powers of DPB and make it more effective for better implementation of the law.

(ii) Under the DPDP Act, wide discretionary powers have been given to the Government by virtue of certain provisions, for example under section 9(4) of the act whereby Data Fiduciaries have been given considerable leeway or exemption in relation to processing of data of children. No basis has been provided for granting such exemption. Giving such wide powers, may result in the Government taking undue advantage of its authority.

(iii) Although Section 38(1) states that the Act shall be interpreted as being compatible with other laws, Section 38(2) mandates that the provisions of the Act will take precedence over any conflicting provisions in other laws. This is contradictory. Therefore, there is a need to synchronise sectoral regulations because this approach may impact certain industries and is hard to interpret, which could ultimately make compliance challenging.

(iv) Many provisions of the Act entail significant rule making by the Central Government.

However, being a nascent player in the area of data protection as compared to developed nations, the Government should take reference from the best practices adopted by the developed nations and other international entities while framing the rules, so as to ensure effective implementation of data security law.

1.12 CONCLUSION

Data Protection and Privacy are best understood as two sides of the same coin, they go simultaneously, especially in today's digital age. The enactment of the "Digital Personal Data Protection Act (DPDP), 2023" has been a watershed moment in the arena of data security. It has sought to make considerable changes so as to effectively secure the personal data of individuals. Many of the provisions of the Act such as those mandating consent requirements, protection of children's data, legitimate uses etc. are groundbreaking as they impose obligations on businesses and organizations to be responsible while handling personal data and also be ready to face consequences in case of breach of data and violations of other significant provisions of the Act. The Act though a significant piece of legislation in the area of data privacy, suffers from certain limitations which may also prove to be challenging in its implementation, especially coupled with lack of awareness at present among the people. Nevertheless, it will be interesting to see how this law heralds a new era of data security and strengthens the privacy of people in the digital era.

REFERENCES

1. J.N. Pandey, Constitutional Law of India, Central Law Agency, 61st edition (2024)
2. MP Jain, Indian Constitutional Law, Lexis Nexis, 9th edition (2024)
3. Sanjay Jain, V.D. Mahajan's Constitutional Law of India, Eastern Book Company, 8th edition (2023)
4. The Information Technology Act, 2000 (Act 21 of 2000), https://www.indiacode.nic.in/handle/123456789/1999
5. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
6. Paulo Campanha Santana, Faiz Ayat Ansari, "Data Protection and Privacy as a Fundamental right: A Comparative Study Of Brazil And India", Vol.9, No.3, Journal of Liberty and International Affairs (2023)
7. Kumar NH, "A Study on Right To Privacy And Data Protection In The Cyber Space",Vol.6,No.4, International Journal of Creative Research Thoughts (2018)
8. Payal Thaorey, "Informational Privacy: Legal Introspection in India", Vol. II, ILI Law Review (2019)
9. How aware and prepared are Indian consumers and businesses to navigate the new era of digital privacy? A survey of India's data privacy landscape. https://www.pwc.in/assets/pdfs/aware-prepared-indian-consumers-businesses-navigate-new-era-digital-privacy.pdf
10. "Anirudh Burman, Understanding India's New Data Protection Law (October 3, 2023) https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en"
11. Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?," Carnegie India, https://carnegieindia.org/2020/03/09/will-india-s-

proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217

12. India Cybersecurity Domestic Report 2023, https://www.dsci.in/resource/content/india-cybersecurity-domestic-report-2023