IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

ADVANCEMENT OF TECHNOLOGY, LACK OF PRIVACY: PRE-REQUISITE OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023.

CA Shagun Kabra and Ms. Khyati Lad

CA Shagun Kabra: Student of SVKM's Jitendra Chauhan College of Law
Ms. Khyati Lad: Student of SVKM's Jitendra Chauhan College of Law

❖ ABSTRACT

The article examines how privacy violations brought about by technological advancements prompted the passage of the Digital Personal Data Protection Act (DPDP Act). It states that technology and the internet have completely changed our lives, making them more efficient and convenient. However, the price that each person must pay for the growth of technology is the erosion of privacy. When we use technology for social media, online shopping, web browsing, cloud storage of personal data, and other activities, we leave digital trails behind. Because our personal information is easily accessible in the digital realm, criminals can more easily identify us and distribute, obtain, and use it fraudulently, which can result in cybercrimes. Therefore, the government passed a new law that mainly governs the protection of personal data in order to address the invasion of informational privacy and safeguard the fundamental right to privacy stated in Article 21. The legislation gives each person the authority to govern their data, including the ability to access, edit, and revoke it. Additionally, data fiduciaries have a need to be more open and disclose their data collection procedures and the reasons behind their data needs. However, even for certain legitimate purposes, no data processing may be done without the individual's agreement. The statute does, however, contain a small number of exclusions that, in specific situations, might free a person from the DPDP Act's requirements. Additionally, unless retention of data is mandated by law, the DPDP Act requires data fiduciaries to delete data upon the withdrawal of express consent or the completion of an intended purpose. The Act also stipulates that the Data Protection Board of India (Board) will impose stringent actions on data fiduciaries in the event of a data breach, after providing them with a chance to be heard. In conclusion, this article explains the salient points of the DPDP Act that individual should be aware of in order to take control of their own personal information. It also explains the rationale behind the need to balance the advancement of new technologies with the escalating concerns about privacy, especially in relation to confidential data that is now easily accessible online.

❖ **KEY WORDS**

Technology, privacy, informational privacy, DPDP Act, data principal, data fiduciary, personal information, consent, artificial intelligence, Board

❖ INTRODUCTION

We are surrounded by and reliant on technology in today's environment as the main uses of technology includes communication, healthcare, education, shopping, banking, transportation, productivity, internet, and keeping records. Not only our personal identity and contact details but also our residential address is to be provided. We willingly provide our debit card and credit card details which includes card number, name of the card holder, expiry month and year of the card and CVV number on different applications and websites while placing order from them. Most of our details are available in virtual verse, it is undoubtedly used for our benefit by us but we at times wouldn't realise how it can be used against us. Majority of the applications and websites put in their terms and conditions of use while we use them for the first time and we agree all the terms mentioned, mostly without even glancing through it. Lately the websites have started sending small pieces of texts to our browser when we visit them known as cookies. It helps in session management and personalization but mainly by accepting cookies we agree for the website to collect our information. Every person currently stores a lot of personal information, such as pictures, medical records, and other crucial data, on a drive or cloud due to the growth of technology and digital data. Weak security measures increase the risk of data leaks, which give hackers access to people's personal information for malicious purposes. As a result, privacy may be at stake.

The rate at which technology is advancing has accelerated recently. Technological advancement is a blessing for the world. It has also made access to entertainment effortless with the help of social media and virtual reality experiences to online gaming and streaming services. It is important to recognise not only the benefits but also the potential drawbacks of the advancement of technology which will allow us to use technology responsibly and use it for the enhancement of humanity.

The major shortcomings of technological advancement are lack of privacy, data breaches and cybersecurity threats.

Before the DPDP Act[1] was brought into action, we had to count on the IT Act[2] and SPDI Rules[3] as the only regulation for data-related activities. Since 2018, the Indian Government was attempting to introduce and implement a central law for data protection and act as an independent data protection law in response to the growing concern of personal data breach.

Eventually, in the year 2023, the Digital Personal Data Protection Bill (DPDP Bill), 2023 was approved by the Lok Sabha on 3rd August, 2023. On 9th August, 2023, the Rajya Sabha passed the DPDP Bill.

[1] Digital Personal Data Protection Act, 2023
[2] Information Technology Act, 2000
[3] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Conclusively, the President of India granted her assent to the same and the Digital Personal Data Protection Act, 2023 was notified and published in the Official Gazette of India.

❖ CONCEPT OF PRIVACY

• RIGHT TO PRIVACY

According to Black's Law Dictionary, 'right to privacy' is a generic term encompassing various rights recognised to be inherent in concept of ordered liberty and such rights prevent government interference in intimate personal relationships or activities, freedoms of individual to make fundamental choices involving himself, his family and relationship with others.[4]

Privacy is a fundamental human right under Article 21 of the Constitution and it is a concept that deals with various aspects of an individual's life and information. Article 21 of the Constitution of India states that no person shall be deprived of his life or personal liberty except according to procedure established by law.[5]

The government uses finger prints and facial recognition technology to maintain records of its citizens and to utilize them legitimately when needed. Electronic gadgets such as laptops, tablets, smart watches and mobile phones also use these technologies. The companies and government agencies collecting these data must have strict rules and regulations for the intermediaries through which these data have been collected. For instance, the use of face recognition software by police cannot be claimed as invasion of confidentiality, as long as it is carried out with sufficient precautions. It is indispensable to take steps to guarantee that the software is only used for positive purpose and that the gathered information should not be exploited. For companies that employ technology to recognize faces derived by artificial intelligence, it is mandatory for them to verify that such technologies are utilised professionally and responsibly, with sufficient protections to protect personal data. These are a few instances where the strict guidelines should be followed by the government agencies, intermediaries and companies while preserving information of the individuals so that their data remains confidential and that their right to privacy is not exploited.

• INFORMATIONAL PRIVACY

Today's world offers a variation of privacy options. However, informational privacy is a new phenomenon as a result of the increase in digital presence and digitalized personal data.

The term "informational privacy" describes a person's ability to decide how and when their personal information is collected, shared, and utilized. Personal Data as per the Digital Personal Data

[4] Black's Law Dictionary
[5] Constitution of India

Protection Act means *"any data about an individual who is identifiable by or in relation to such data"*.[6]

In the landmark Aadhar case[7], the main arguments of the petitioners regarding privacy were that such project design necessitates the individuals to part with biometric information and the authentication process can be easily abused. The data relating to different undertakings over the life of the individual is connected to a central database which may sanction the state to profile citizens, keep a track on their movements, examine their habits and try to influence their behaviour and decisions. The question before the court was whether the Act is unconstitutional because it excruciates at the fundamental right to privacy of the individual.

It was held that the Aadhar Act does not violate the right to privacy when a person agrees to share his biometric data.

- **IMPACT OF EMERGING TECH ON PRIVACY**

The emergence of artificial intelligence (AI), biometrics, machine learning, the Internet of Things, and other innovations has led to a rise in task performance and the digital presence of personal data. Others can quickly identify that person thanks to the information that has been gathered and saved online.

Lately, the significant increase in the use of AI is not only a boon but also a curse especially when it comes to data privacy as it can allow hackers entry to any company's network, user information, datasets and apps through their interface. Hence, businesses utilising AI must think about issues including the lifetime of the data and how it is preserved, utilised and who has access to it.[8]

Also, the advertisements for related products, articles and news appear instantly on search engines and social media feeds when we conduct online searches, have a telephonic conversation or in-person conversation about any topic or product using devices with internet access.

The growing amount of personal data being collected and stored leads to vulnerabilities that can result in data breaches, which can cause identity theft, financial fraud, reputational damage, and other issues.

The DPDP Act was passed to provide a legislative framework for regulation in order to address all the issues pertaining to privacy that have arisen as a result of people's growing online presence.

[6] Sec 2(t) of DPDP Act, 2023
[7] Justice K.S.Puttaswamy(Retd) & Anr vs Union of India, (2015) 8 SCC 735.
[8] Artificial Intelligence, Data Analytics and Cyber Security, Institute of Company Secretaries of India

❖ OVERVIEW OF THE ACT

- **OBJECT AND ITS APPLICABILITY**

The DPDP Act specifically applies to the processing of digital personal data only for specified lawful purpose for which the individual has given his consent.

The applicability of the DPDP Act is within the territories of India where personal data is collected in digital form or in non-digitalized form which is subsequently digitalized. It will also apply outside India if processing is connected with any activity related to the offering of goods or services to data principals in India.[9]

However, the DPDP Act excludes from its application the processing of personal data by an individual for any personal or domestic purpose and any data that is made publicly available by the data principal or any other person who is obligated under any law.[10]

The DPDP Act provides exemptions from certain provisions under certain circumstances where personal data is processed for enforcing legal rights, prevention, detection, investigation, or prosecution of any offence or contravention, scheme of compromise, arrangement, merger, amalgamation, etc.
It is also exempt if any contract is entered into with any person outside the territory of India by any person based in India.

Additionally, the Central Government and the State Government are also exempt from the applicability of the DPDP Act under certain circumstances, and the Central Government may notify certain data fiduciaries, including start-ups, that are exempt from certain provisions of this act.

- **SALIENT FEATURES**

1. The legislation governs the processing of personal data exclusively for purposes that are lawful. The information provided willingly by the data principal for a specific purpose, or to satisfy a legal requirement, or to comply with a court ruling, decree, or order may be processed by a data fiduciary. Additionally, data processing is involved in responding to medical emergencies, offering medical care or other health services, and taking any necessary action to guarantee someone's safety or assistance.

[9] Sec 3(a) and (b) of DPDP Act,2023.
[10] Sec 3(c) of DPDP Act,2023.

If previously consented, even the State and any of its instrumentalities may process personal data to offer any benefit, subsidy, certificate, permit, or license to data principal.[11]

2. In accordance with this DPDP Act, the data principal's express consent must be obtained before processing personal data. The data fiduciary would notify the data principal about the personal data and the reason it is processed in order to comply with this.
   It should be remembered that consent must be freely given and should be explicit, specific, informed, unconditional, clear-cut, and revocable.[12]

3. The DPDP Act safeguards data principals by declaring that if any part of consent violates any law for the time being in force, it will be void to the degree of the infringement.[13]
   For instance, When Mr. A download the fitness app X, X requests permission to view his health details, location and contact list. Mr. A expresses his approval. Since access to the location and contact list is not necessary, his consent will only be granted with respect to his health details.
4. Data principals has been given a right to withdraw the consent under the DPDP Act. In this scenario, data fiduciary shall cease processing of the personal data within reasonable time unless processing is required or authorised under this act or any other law for time being in force.[14]

5. In addition, unless retention is necessary for compliance with any currently enacted laws, the personal data of the data principal is deleted upon consent withdrawal or the completion of the intended purpose, whichever comes first.[15]

6. Nevertheless, there is a cost associated with the right of revocation that the data principal must pay.
   For instance, if a bank customer asks for their loan information to be removed from the credit information company's database, they can eventually lose access to the banking system.[16]

7. In addition to the rights listed above, data principals also have the right to nominate, access, correct, and remedy their grievances over personal information kept by the data fiduciary at their disposal.[17] However, before addressing the Data Protection Board of India, the data principal should exhaust all possible avenues for resolving the complaints.[18]

[11] Sec 7 of DPDP Act,2023.
[12] Sec 6(1) of DPDP Act,2023.
[13] Sec 6(2) of DPDP Act,2023.

[14] Sec 6(6) of DPDP Act,2023.
[15] Sec 8(7)(a) of DPDP Act,2023.
[16] By Suraksha P, Aashish Aryan & Gayatri Nayak, 2024, Banking access may be at risk if you seek to delete credit data
[17] Sec 12(2) and Sec 14 of DPDP Act,2023.
[18] Sec 13(3) of DPDP Act,2023.

8. The data principal is assigned certain responsibilities also. Some of these include not impersonating another individual while supplying personal data, submitting legitimate information without suppressing facts, and not filing fraudulent or frivolous complaints.[19]

9. The Central Government prohibits by notification data fiduciaries from transferring personal information to countries outside of India for processing.[20] This is one of the steps done to protect the rights and interests of the data principal.

10. The legislation mandates data fiduciaries to notify the Board and affected data principals of any personal data breaches, in addition to other rights and obligations outlined in the DPDP Act.[21]

11. The Board has the same power as vested in a Civil Court. It also performs numerous functions, including immediate remedial or mitigation steps in the event of a personal data breach, imposing penalties, determining adequate grounds to proceed with an inquiry, issuing interim orders, and issuing a warning or cost in the case of frivolous complaints.[22]

12. If any person is aggrieved with the Board's orders or directions, they can file an appeal with the Appellate Tribunal within 60 days from date of receipt of order or directions, under the DPDP Act provisions. The appeal must be decided within 6 months from the date on which appeal was presented to him by confirming, amending, or setting aside the order appealed.[23]

    These are some of the many characteristics of the act that provide the data principal with further protection against data breaches and the ability to manage his personal data.

- **LIABILITY UNDER THE ACT**

After giving the individual, a chance to be heard, the Board may impose a monetary penalty as outlined in the Schedule if the investigation concludes that the person's breach was serious.[24]

The Schedule lays out various financial penalties for various violations in addition to a general penalty of up to Rs. 50 crores. The Schedule specifies a maximum penalty of Rs. 250 crores which is mentioned for data fiduciaries who fail to fulfil their commitment to implement adequate security measures to avoid the compromise of personal data.[25]The penalty may also be increased by the Central Government by notification, although it cannot be increased above double the amount specified in the Schedule.[26]

[19] Sec 15 of DPDP Act,2023.
[20] Sec 16(1) of DPDP Act,2023.
[21] Sec 8(6) of DPDP Act,2023.
[22] Sec 27 and Sec 28 of DPDP Act,2023.
[23] Sec 29 of DPDP Act, 2023.
[24] Sec 33(1) of DPDP Act,2023.
[25] The Schedule of DPDP Act, 2023.
[26] Sec 42(1) of DPDP Act,2023.

When calculating the appropriate penalty amount, the Board will consider the type, extent, and severity of the breach in addition to its duration, repetition, realized gain or loss, and the nature of personal data that was compromised.[27]

❖ CRITICISM

There are some situations where the legislation provides an exemption. However, the exception may result in data collection, processing, and retention beyond what is required. This would constitute a violation of an individual's fundamental right to privacy.

Furthermore, the DPDP Act acknowledges the data principal's right, while it does not yet provide sufficient details regarding how that right will be exercised.

The lack of clarity in the regulation surrounding the governance of data that would be transferred online is one of the primary problems. Though, the Central Government may choose which nations receive personal data, but it is unclear how the government would control it.

❖ RECOMMENDATION

Public education about cyberthreats, cybersecurity, privacy rights, data breaches, and data protection is necessary, according to the government. The DPDP Act, 2023, should also be made known to the public so that they can use it to stop the dangers and breaches they are currently experiencing.

The provision of the DPDP Act should also include right to erase individual's personal data. For Instance, the individual's private data that has become public and is available on different portals due to a particular company or website, provision to remove that data from all the portals should be available. After removal of such data it should be intimidated to the complainant.

❖ CONCLUSION

In today's world, we share personal information including our identity, biometrics, pictures, location, contact number and email address especially on different shopping, food delivery, government-based applications and websites. It is essential regarding the private information of their clients and website users that these businesses and intermediaries must adhere to stringent laws and guidelines. Also, protecting the security and privacy of sensitive data is essential for the ethical creation and utilisation of AI.

The DPDP Act greatly aids in mitigating the problems associated with technological growth and invasions of privacy, which are essential in this era. However, there are certain barriers that should be considered. By defining rules for data collection, processing, and revocation, the DPDP Act gives data principals more control and protection over their personal data and upholds their fundamental right to privacy.

[27] Sec 33(2) of DPDP Act,2023.

Since regulations have not yet been created, the DPDP Act's efficacy will rely on how they are put into practice. Additionally, the legislation would need to be updated and examined on a regular basis to address modern violations.

Furthermore, because data is transferred internationally, international cooperation is required to address privacy problems.

Therefore, the DPDP Act establishes the foundation for safeguarding individuals who may be impacted by breaches of personal data and granting them the ability to manage their own data. However, the act's effectiveness won't be known until it is put into practice.

❖ REFERENCES

Artificial Intelligence, Data Analytics and Cyber Security, ICSI, https://www.icsi.edu/media/webmodules/Academics/Elective_Paper_AIDA_CS.pdf

https://articles.manupatra.com/article-details/A-Paradigm-Shift-In-Data-Protection-Analyzing-The-Digital-Personal-Data-Protection-Bill-In-The-Context-Of-India-s-Privacy-Landscape

https://iapp.org/news/a/the-indian-supreme-courts-aadhaar-judgement-a-privacy-perspective/

https://legislative.gov.in/constitution-of-india/

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2273074

https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022

The Digital Personal Data Protection Act, 2023, No. 22 of 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf