ISSN (O): 2584-2196

# INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND EXPLORATION

**Volume 2| Issue 3**

**2024**

# DATA PROTECTION AND PRIVACY LEGAL-POLICY FRAMEWORK IN INDIA IN REFERENCE TO THE DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT, 2023: A COMPARATIVE STUDY BETWEEN INDIA AND AUSTRALIA

***Sulagna Talukdar***

*2nd Year BA LL.B Student of Shyambazar Law College, University of Calcutta.*

## ABSTRACT

*Development of a productive data protection and privacy framework is necessary for the progress of a country. For, it has become common among the organizations to increasingly accumulate personal information and advancing breach of privacy concerns. India is acknowledged as the outsourcing hub by countries like UK and US which consider data protection as a fundamental right of their citizens. Now, whatever laws are there that prevent illegal use of personal and private data, till now Indian citizens are dependent on them only. The Digital Personal Data Protection (DPDP) Act, 2023 has been enacted after a lustrum of deliberations. This paper confers about whether this seemingly endless period of deliberations resulted in a "good" law and protects personal data adequately. Furthermore, whether it properly balances, as the preamble to the law states, "the right of individuals to preserve and safeguard their personal data" on one hand and "the need to process such personal data for legitimate purposes" on the other. Through this paper, the author will try to find out how India is lacking behind Australia in terms of Data Protection and Privacy laws and the need to advance itself in pertinent implementation techniques.*

**Key Words:** *Data Protection, Breach of Privacy, the Digital Personal Data Protection Act 2023, Fundamental Right, Information.*

## 1. INTRODUCTION

The global interest in data protection legislation is growing rapidly due to the ease with which sensitive personal information can be shared today. Consequently, it's crucial for organizations to implement effective measures to safeguard personal data. Governments and companies around the world have implemented numerous preventative measures to defend information against attackers. Despite advancements in technologies like IoT, Machine Learning, and Artificial Intelligence,

ensuring data protection remains a significant concern, posing a daunting challenge for the future[1]. Cybercrimes are being amplified with activities like identity theft, fraudulent transactions, leak of private information, harming a person's reputation, computer viruses and ransomware in this age and date. Nowadays, we are often asked to provide personal information like name, date of birth, email, mobile number and many more before registering in various online platforms. Downloading an app requires permission to access storage, contacts, microphone, cameras, etc. We being ordinary people are not cognizant about these and we do not know anything about how a company uses our data or information that we have provided. Hence, it is high time to make sufficient laws and prevent the data hackers from committing data theft. India can be seen to take interest regarding the influence of data protection laws passed in other countries through which this has been discover that India has minimal restrictions and Australia has some restrictions. Through the use of such a kind of comparative study, India can achieve the goal of proceeding forward.

## 2. RESEARCH METHODOLOGY

This paper is of descriptive nature and the research depends on secondary sources for the in-depth examination of the Privacy Laws. Secondary sources of information like PDFs, newspapers, journals, and websites are used for the research.

## 3. DIFFERNECE BETWEEN DATA AND INFORMATION

There is a huge misconception that usually confuses people between Data and Information. But both of these are the same things. Data are simply the facts that can be recorded like text, audio, video, etc.[2] whereas information is a processed data which holds a meaning, but the raw unprocessed data or simply the data as such has no meaning. When we store the data inside the database, we do it neatly and store it in a well-organized manner. Such tidied work attracts data collectors and helps them to do data breach with a lot of ease.[3]

[1] Dr. Yadav, Network security and its role in controlling cyber-crimes, researchgate.net,(Last accessed on 10th April 2024), https://www.researchgate.net/publication/354006973_NETWORK_SECURITY_AND_ITS_ROLE_IN_CONTROLLING_CYBER-CRIMES
[2] Jack Vaughan, What is data management and why is it important?, Tech Accelerator, (Last accessed on 11th April 2024), https://www.techtarget.com/searchdatamanagement/definition/data-management
[3] GeeksforGeeks, https://www.geeksforgeeks.org/sql-views/, (Last accessed on 11th April 2024)

## 4. LAWS AND POLICIES OF DATA PROTECTION AND PRIVACY (INDIA AND AUSTRALIA)

The Indian Parliament passed the Digital Personal Data Protection (DPDP) Act[4] on August 2023. A committee of experts initially drafted a version of the bill, which underwent a public feedback phase in 2018. Following this, the government formally introduced the bill in Parliament in 2019. Subsequently, a parliamentary committee analyzed the 2019 version and issued its report in December 2021. However, the government later withdrew this bill. In November 2022, a fresh draft, titled the Digital Personal Data Protection Bill, 2022, was published for public consultation.

The 2023 act represents the second iteration of the bill introduced in Parliament and the fourth overall version. It's important to note that privacy rights are safeguarded by the Constitution of India and also addressed in the Information Technology Act, 2000. Property rights, on the other hand, are covered by various legislations such as the Indian Contract Act, 1872; the Copyright Act, 1957; and the Indian Penal Code, 1860.

Additionally, the Ministry of Communication and Information Technology in India has implemented privacy regulations known as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Lok Sabha Secretariat, 2013). These rules mandate businesses to handle the collection, processing, and storage of personal data responsibly.[5]

In Australia, data protection and privacy regulations are a combination of federal and state laws. The Federal Privacy Act of 1988, along with the principles of privacy, extends to Commonwealth Government agencies, Australian Capital Territory Government agencies, and private sector companies with an annual turnover of at least AUD 3 million. Additionally, Australian states have their own data protection legislation. Examples include the Information Privacy Act of 2014 for the Australian Capital Territory, the Information Act of 2002 for the Northern Territory, the Personal Information Protection Act of 2004 for Tasmania, the Privacy and Personal Information Protection Act of 1998 for New South Wales (NSW), the Privacy and Data Protection Act of 2014 for Victoria, and the Information Privacy Act of 2009 for Queensland.

[4] MeitY, (Last accessed on 11th April 2024) https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf ,
[5] Dla Piper(2014a) Data Protection Laws of the World, (Last accessed on 11th April 2024) https://www.dlapiperdataprotection.com/system/modu,

Furthermore, various other laws influence data protection and privacy for specific data or activities. These include the Telecommunications Act of 1997 at the federal level, the National Health Act of 1953 at the federal level, the Health Records and Information Privacy Act of 2002 in NSW, the Health Records Act of 2001 in Victoria, and the Workplace Surveillance Act of 2005 in NSW. [6]

## 5. STATUS OF DATA PROTECTION, PRIVACY RIGHTS AND PROPERTY RIGHTS IN INDIA

The Supreme Court has established in various cases that Article 21, which guarantees the right to privacy, is encompassed within the right to life and personal liberty. It asserts that no individual can be deprived of their life or personal liberty except through procedures established by law. However, constitutional rights cannot be invoked against private entities or organizations; they can only be invoked against state-owned enterprises or the state itself. The Information Technology Act of 2000 includes provisions addressing cyber contraventions (Sections 43(a) to (h)) and cyber offenses (Sections 65 to 74). Cyber contraventions encompass actions such as unauthorized access to and extraction of data from computer systems or networks, which can result in civil prosecution in India. Cyber offenses involve activities like intruding into computer source code, hacking with the intention to damage systems, banking fraud, cyberbullying, and breaching privacy, all of which can lead to criminal prosecution under the IT Act. Furthermore, the IT Act outlines penalties for these offenses[7]. Under the regulations of the IT Act, any network service provider or intermediary bears responsibility for any misuse of third-party information and is accountable for failing to exercise due diligence to prevent such misuse. An intermediary, as defined by the IT Act, refers to an entity that acts on behalf of another entity and engages in activities such as receiving, storing, transmitting, or providing services related to electronic messages. Consequently, an outsourcing company may be held liable as a service provider under these provisions. Moreover, the IT Act extends its jurisdiction extraterritorially, encompassing offenses and contraventions committed beyond India's borders.

Article 300A of the Indian Constitution safeguards individuals from being deprived of their property except by lawful authority. However, this protection applies solely against the State and cannot be invoked against private entities. Additionally, for this right to be enforced, the relevant

[6] Dla Piper(2014c) Data Protection Laws of the World, , (Last accessed on 11th April 2024) http://www.dlapiperdataprotection.com/system/modu
[7] Dot.gov.in, (Last accessed on 11th April 2024) https://dot.gov.in/sites/default/files/itbill2000_0.pdf,

data must be recognized as the individual's property[8]. The Indian Copyright Act of 1957 safeguards Intellectual Property (IP) rights, covering various forms such as artistic, dramatic, musical, literary, and cinematographic works. Notably, computer databases fall within the scope of literary works. Therefore, copying and distributing a computer database can constitute a violation of copyright. The Copyright Act, 1957 provides both civil and criminal remedies for such breaches[9]. However, it's important to note that the Copyright Act does not draw a clear distinction between data protection and database protection. Data protection primarily focuses on safeguarding the personal information of individuals, while database protection is aimed at preserving the originality and investments made in compiling, verifying, and presenting databases. The Indian Penal Code (IPC), 1860 can be utilized as an effective tool to prevent data theft. Under the IPC, theft, misappropriation of property, and criminal breach of trust are punishable offenses, carrying penalties such as imprisonment and fines. Misappropriation of property, as defined in the IPC, applies specifically to movable property and encompasses tangible assets of all kinds, excluding those permanently attached to land. Given that computer databases are movable in nature, they can thus be protected under the IPC to a certain extent (Law Commission of India, 1997)[10].

## 6. COMPARATIVE STUDY BETWEEN INDIA AND AUSTRALIA

A concise comparative analysis of legal provisions:

- ***Definition of Personal Data***: In India, personal data pertains to information that can identify a natural person and is accessible to a corporate entity, while in Australia, it encompasses any information or opinion about an identifiable individual.
- ***Definition of Sensitive Personal Data***: In India, sensitive personal data includes financial information, health records, passwords, sexual orientation, biometric data, etc. In Australia, it refers to genetic information, racial or ethnic origin, political opinions, religious beliefs, health information, criminal record, membership of a trade union, etc.
- ***Data Protection Authority***: India lacks a specific Data Protection Authority, while in Australia, the Privacy Commissioner serves as the national authority.

[8] Singhal, M.L (1995),( Last accessed on 11th April 2024) http://ijtr.nic.in/articles/art41.pdf
[9] Copyright.gov.in , (Last accessed on 11th April 2024), http://copyright.gov.in/documents/copyrightrules195
[10] Law Commission of India (1997), One Hundred
Fifty-Sixth Report on The Indian Penal Code,
Volume II, August 1997, (Last accessed on 11th April 2024) https://lawcommissionofindia.nic.in/101-

- ***Presence of Data Protection Officers***: In India, every corporate entity must appoint a grievance officer, whereas in Australia, while not mandatory, having such officers is strongly recommended for organizational development.
- ***Data Collection and Processing***: Indian corporate entities are liable for damages, while Australian businesses ensure accuracy in collected personal information and gather only essential data for business purposes.
- ***Data Transfer***: In India, consent is required from the provider for transferring sensitive personal information, while in Australia, data can be disclosed under certain legal provisions.
- ***Security***: Both countries mandate fair security practices for data protection.
- ***Fines and Penalties***: In India, civil penalties can amount to up to 6 Crore, with criminal penalties including imprisonment for up to 3 years or a fine up to 6 Lakhs. In Australia, fines for failing to protect personal data can reach up to AUD 340,000 for individuals and AUD 7 million for corporations.
- ***Online Privacy***: India's IT Act and DPDP Act 2023 address civil and criminal offenses related to cyber-crimes, though there is no specific Privacy Law. In Australia, privacy laws regulate the collection of location data, use of cookies, etc., under the Privacy Act and State/Territory privacy laws.[11]

## 7. IT ACT, 2000

Data security regulations in India are sourced from various channels, with the IT Act 2000 being the most comprehensive. Inspired by the United Nations Commission on International Trade Law of 1966, the IT Act 2000 serves as the primary framework for cybersecurity in India. It encompasses a wide range of regulations addressing cybercrimes like intellectual property rights violations, hacking, and data breaches. Despite its extensive provisions, the existing legal landscape falls short in adequately addressing the complexities of data security. Only sections 43A, 69, 72, and 72A of the IT Act 2000 directly pertain to data protection issues[12].Under Section 43A of the IT ACT 2000, individuals affected by insecure data practices of data collectors or handlers can hold them accountable. Penalties including fines and compensation may be imposed, with no specified upper limit for compensation. Section 69, added to the IT ACT in 2008,

[11] Dla Piper(2014) Data Protection Laws of the World, (Last accessed on 11th April 2024) https://www.dlapiperdataprotection.com/system/modu ,
[12] Legal Service India(2021), Data Protection Law In India, (Last accessed on 11th April 2024) https://www.dlapiperdataprotection.com/system/modu ,

empowers authorities to shut down or ban websites or applications posing threats to India's image or relations. Breaches of confidentiality are addressed under Section 72, with penalties including up to two years imprisonment, a fine of one lakh rupees, or both. Section 72A concerns the unauthorized disclosure of user data by service providers, with penalties of up to three years imprisonment, a fine of up to five lakh rupees, or both[13].With several sections, IT ACT 2000 is a much vast act, but it is not very robust in the present time. The absence of laws on Domain Names, silence about taxation on online transactions etc. are some of its shortcomings. It contains several Loopholes and doesn't have enough capability to tackle the present and upcoming cyber threats and crimes. [14]

## 8. THE DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT

Personal data involves the information that relate to an identifiable person and it is supposed to be handled well by the businesses and the organizations to provide goods and services. This refining of personal data helps to grasp individual preferences, which can be advantageous for personalized customization, targeted advertising, and providing recommendations. It can also perform well in law enforcement attempts. However, if not regulated, the processing of personal data can have negative consequences on individual privacy. Unchecked processing could expose individual's potential harm, including financial losses and defamation. Thus, it has became critical for the country to come up with an act that can regulate data protection. Currently Information Technology (IT) Act, 2000, is the act regulating personal data and data protection. However in 2017, the government established a panel of experts chaired by Justice B. N. Srikrishna to investigate issues concerning data protection in the country. The panel presented its report in July 2018. Taking into account the panel's advices, the Personal Data Protection Bill of 2019 was introduced in the Lok Sabha in December 2019.The bill was then referred to a Joint Parliamentary Committee, which delivered its report in December 2021. However, in August 2022, the bill was withdrawn from Parliament. Subsequently, in November 2022, a Draft Bill was made available for public feedback. Finally, in August 2023, the Digital Personal Data Protection Bill of 2023 was introduced in Parliament and subsequently got implemented. The Digital Personal Data Protection Act 2023 stands as a concise and well organized legal framework that reflects India's view concerning data protection principles in relation to the functions of both individuals and

[13] Legal Service India.com, (Last accessed on 11th April 2024) https://www.legalserviceindia.com/articles/cddisp.htm
[14] Legal Service India.com, (Last accessed on 11th April 2024) https://www.legalserviceindia.com/articles/cddisp.htm

businesses. It sheds light on the fundamental aspects of the Act that organizations must consider prior to embarking on their endeavours towards achieving privacy compliance.

## 9. CONCLUSION

India has taken significant steps towards enhancing data protection and privacy through a range of legal and policy initiatives. Research highlights that within India's legal-policy framework, certain privacy and property rights afford a degree of data protection and privacy. Notably, the Digital Personal Data Protection Act of 2023 is a key legislation, supplemented by various other laws such as the Constitution of India, Information Technology Act of 2000, Indian Contract Act of 1872, Copyright Act of 1957, and Indian Penal Code of 1860.

However, it's evident that India's current legal-policy framework for data protection and privacy has limitations, particularly when compared to countries like Australia. Some disparities between India and Australia include the absence of specific laws and regulations in India regarding the management of cookies, location data, and behavioral advertising, as well as the lack of a comprehensive legal-policy framework in India to address data protection and privacy concerns related to electronic marketing, unlike Australia's SPAN Act of 2003.

Furthermore, India lacks a dedicated National Data Protection Authority similar to Australia's Privacy Commissioner. Strengthening India's legal-policy framework for data protection is crucial, especially considering the significant role data protection plays in outsourcing arrangements. Foreign investors often entrust sensitive data such as confidential customer information and trade secrets to India for back-office operations. Enhancing data protection measures can safeguard against potential mishaps, contributing to the stability of India's economy.