18

A COMPARATIVE ANALYSIS OF THE INDIAN DATA PRIVACY ISSUES IN THE DATA PROTECTION ACT VIS-A-VIS RIGHT TO PRIVACY IN INDIAN CONSTITUTION

AASTHA NARULA

ASSISTANT PROFESSOR, DEPARTMENT OF LAW, MAHARAJA AGRASEN INSTITUTE OF MANAGEMENT STUDIES, NEW DELHI

Abstract

The Digital Personal Data Protection Act, 2023 replaced the Personal Data Protection Act (PDP), which was initially proposed in 2019 and was finally passed by Rajya Sabha on 9 August 2023 by voice vote. A preliminary examination reveals that the Act regulates processing, which covers the gathering and storing of personal data as well as its modification, dissemination, removal, and destruction. The DPDP Act also establishes a compliance framework, including the formation of a Data Protection Board. The creation and use of systems for data transfer between devices has increased the need for updated data protection and privacy laws both internationally and in India. The Puttaswamy case in 2017 led to the acceptance of privacy as a fundamental right under Article 21 despite the absence of an official definition in the Indian Constitution. A concise yet comprehensive account of India's data protection laws, developments, and case laws are discussed in this paper. This paper also looks at India's IT Act, which controls data privacy, and it paints a picture of why data privacy has to be protected.

Keywords: *Data Privacy, Fundamental Rights, Indian Constitution, Data Protection.*

Introduction

What images do you have in your head when you think about privacy? Perhaps a setting where you can engage peacefully with the people you desire or one where you can guard against the leak of your private information. Today, privacy encompasses safeguarding personal information, avoiding intrusions, and ensuring the security of digital information transferred over the internet. The issue of data privacy must be resolved immediately in order for consumers to enjoy their fundamental right to privacy and safeguard themselves against unauthorized use of their data as the Indian economy nears the pinnacle of technological breakthroughs.

The privacy's right was ultimately incorporated in Part III of the Constitution of India after the matter of *Kharak Singh vs. State of U.P.*, when a six-judge court ruled that the Constitution of India does not protect privacy of any person.[1] In contrast, the Apex Court, which was composed of a 9-judge bench, accepted the privacy as a fundamental right later.[2]

After the J. Puttaswamy judgement, the Union government appointed 10-member committee to indulge in the data protection-related problems in response to calls for comprehensive data protection rules. The committee's final proposal was the PDP Bill of 2019. Despite being designed to secure and protect the privacy of India's personal information across the nation, the plan drew criticism for disregarding crucial concerns and providing significant exemptions to a small number of enterprises.

The Digital Data Protection Act of 2023, an upgraded version of the PDP Bill of 2019, was the most current proposal to achieve this. On 03rd August, 2023, the DPDB was reintroduced into the Lok Sabha by Ashwini Vaishnaw, Electronics and Information Technology's Union Minister and was finally passed by Rajya Sabha on 9th August 2023.

Meaning & Contents of Privacy

Privacy is an individualized and a subjective concept. 'Privatus' its Latin name, connotes seclusion from the outside world. Steven Lukes makes the case that the concept of individuality has shaped how the concept of privacy has developed in his essay titled "The Meanings of 'Individuality"'. Individualism is defined as placing a strong emphasis on a person's moral value, which might refer to their moral position, political philosophy, ideology, or sociological viewpoint. According to the individuality thesis, every person has the right to all freedoms as their creator gave them existence, including the right to privacy.[3] According to John Locke, privacy and freedom go hand in hand. Because he could only provide this freedom at times of conflict, Locke argued that someone who lived under the bounds of a social contract is free within those constraints. Privacy allows everyone to be left alone in a holy area.

For individuality to grow and be saved, privacy is necessary. According to Jeffrey Reiman, respecting one's moral claim to autonomy and ownership of one's physical and psychological reality is what is meant by privacy. Even when a person's inner sanctum or designated private place is off limits, their contacts with other people in society still have an effect on some aspects

[1] Kharak Singh vs. State of Uttar Pradesh, 1964 SCR (1) 332.
[2] Justice KS Puttaswamy (Retd.) vs. Union of India, (2017) 10 SCC 1.
[3] Steven Lukes, *The Meaning of "Individualism"*, 32, Journal of the History of Ideas, 45 (1971).

of their privacy because during these exchanges, a person's individuality and autonomy are constantly called into doubt. The establishment of facets of social life that require a person to give up his right to free will is another way that the state and non-state institutions put pressure on people.

Salmond contends that a right is an interest that is protected by a law of rights. Any interest deserves attention and should never be neglected. Salmond's definition of a right is that privacy is a fundamental interest held by all individuals, therefore it must not only be recognized but also protected against outsiders and governmental intervention.

- The earliest recognized privacy thread has to do with physical or spatial privacy, especially in relation to space. This geographical privacy safeguards a person's right to personal space inside a certain geographic or demographic area, such as their home. In this instance, privacy as a person's sacred space is extremely effectively preserved. In other terms, privacy is defined as "the right of a person to be let alone" by Justice Cooley of the USA. For instance, it is appropriate to apply the protection of constitutional liberty to certain types of privacy.
- The ability to make certain significant decisions and individual choice are what privacy largely has to do with. This idea of privacy is more concerned with a person's ability to make decisions for themselves than it is with physical limits. Along with the freedom to make choices, this also includes the authority to determine how those choices will be carried out. Using technology to efficiently exercise one's right to free speech and expression, for instance.

The crucial protections are provided by article 19, 21, and 25 of the Constitution of India. For the first time, the court acknowledged privacy as a right in *MP Sharma vs. Satish Chandra*.[1] The Criminal Procedural Code of 1973's provision on search and seizure was contested on the grounds that it violated the petitioner's fundamental rights as guaranteed by the Indian Constitution. The court concluded that no person's constitutional rights can be infringed during a search and seizure procedure.

In *Kharak Singh vs. State of UP*, rule 236 of Chapter XX of the UP Police Regulation was questioned.[2] The court asserted that when someone knocks on the petitioner's door in the middle of the night, it violates his right to personal liberty, which is protected by article 21 of the Constitution of India. The right to privacy is thus protected by Article 21 in regards to one's house but not in connection to a public context.

The Indian Constitution implicitly preserves some regard for individual autonomy, but only in part. When interpreting the Constitution, Justice Krishna Iyer said in *Gobind vs. State of MP* that our contemplation cannot be only of what has been but also of what may be.[3] Privacy has numerous elements, and one should proceed with caution while analyzing the allegations on a case-by-case basis, Justice Matthew added. Clearly, privacy has a big impact on people. It is therefore related to and overlaps with the notion of liberty.

International Conventions governing Right to Privacy

The EU's regulations governing privacy and human rights are both significantly impacted by the General Data Protection Regulation (GDPR). The transmission of personal data outward to the European Economic Area (EEA) and the European Union (EU) is also covered. The GDPR's main goals are to provide consumers more control and ownership over their personal data and to make regulatory compliance easier for companies with international operations. Following its adoption on April 14, 2016, the GDPR came into force on May 25, 2018. The GDPR has immediate legal effect, is legally binding, and gives member states the authority to change any provisions as they see fit because it is a regulation rather than a directive.

The GDPR's Article 17 and Recitals 65 and 66 both include the right to be forgotten. It stipulates that the controller must abide by the data subject's request to have all personal information pertaining to them destroyed without undue delay in a number of situations.

Despite these rules, a more thorough legislative framework is still required for international data transfers. This is due to the lack of uniformity among various regulatory frameworks and the fact that many nations do not have laws that effectively safeguard personal data. A carefully built legal framework for cross-border data transmission should get high attention given the quickly expanding volume of international data flows and the potential for misuse in terms of national security, data breaches, and privacy problems. The purpose of such a framework is to ensure that personal data is properly protected during transmission and is not vulnerable to misuse or exploitation.

Regardless of how stringent or lenient the regulatory framework for cross-border transfers may be, it is more crucial that the foreign nations taking part in the transfer arrangements make it their responsibility and duty to take all necessary technical, administrative, or social measures to guarantee that the data they collect from the other country is safe and protected and that they comply with all the due diligence requirements of the other country's law. By acting responsibly, the foreign nation may help build confidence between nations so that they may engage in more and more trade internationally without worrying that their data would be hacked or exploited. India may conduct engagement programs with various stakeholder groups in order to achieve this, which might help in understanding their objectives and potential challenges with cross-border data transfers. This plan would enhance the capability of the other stakeholders and enable a broader, more inclusive environment for cross-border data transfers across stakeholders while addressing the protection of the transferred data.

[1] MP Sharma vs. Satish Chandra, (1954) SCR 1077.
[2] *Supra* note 1.
[3] Gobind vs. State of MP, (1964) 1 SCR 332.

Why There's a Need to Secure Data Privacy?

In his statement "Data is the new oil", Clive Humby compares data to crude oil that must be handled according to needs and requirements. Similar to this, managing data in accordance with organizational rules is necessary for it to be valuable. The increased amount of data we are starting to store online, in cloud storage, on devices, etc poses a number of risks that could lead to a breach of data privacy. Organizations have been exploiting Clive's statement for the last few years due to the intrinsic worth of data, which can be used to target clients who are likely to be interested in their goods while also being misused by hackers who can quickly change or erase such data.[1]

Think of a situation where we are browsing a website when a pop-up message prompts us to agree to the site's cookies and privacy statement in order to continue. By accepting the conditions, we consent to the firm using our information including our location, email address, and other specifications mentioned therein and to share it with other applications and websites.

Who is responsible for protecting citizen data from MNCs and hackers? The names, addresses, bank account numbers, and nominee information of Employees Pension Scheme recipients may be found in millions of papers that are freely accessible online without encryption, according to Bob Diachenko, a journalist and cyber security researcher based in Ukraine. Additionally, research from the Dutch cyber-security firm Surfshark claims that out of the 14.9 billion breaches that have occurred worldwide since 2004, 255 million of them have been caused by users from India, accounting for a total of 6,74,85,000 breaches in the first quarter of 2021.

The privacy of Indian citizens must be taken into account by legislators while granting businesses and other economic participants access to data. This is done to encourage new business ventures and innovation in India, which must be regulated and supervised by particular organizations. This is due to India's government now revising the country's data protection laws after the previous Personal data protection bill, 2019, was withdrawn.

Statutory Safeguard as to Data Privacy in India

The IT Act of 2000 and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011 (hereinafter SPDI Rules) have served as India's main data protection laws in the absence of separate data protection legislation. The IT (Intermediaries Guidelines and Digital Media Ethics Code) Rules of 2021 are one of several changes made to the IT Act. This has been done in order to skilfully address issues brought on by cybercrimes as well as other issues relating to data privacy in recent years.

Information Technology Act, 2000

- Altering, destroying, or obtaining unauthorized ingress to a system or network of computer is punishable by the imprisonment up to 3 years or fine up to ₹2 lakh or both.[2]
- The Union or State government may direct a government agency to intercept, track, or decode data sent from a computer device if doing so may endanger India's integrity or sovereignty or damage relations with other friendly countries. Such a person faces the possibility of receiving a fine, a jail sentence of up to seven years, or both if they ignore the government's demands.[3]
- The Union or State government may, in certain situations, prevent the transmission of any information if doing so may harm the sovereignty, integrity, or defence of the nation or the relationships with other friendly states. The Supreme Court finally recognized it as an essential protection for society and affirmed its constitutional legality, despite the fact that the people had fiercely opposed the 2008 change to this part of the Act.[4]

Indian Contract Act, 1872

According to the Indian Law of Contract, revealing that information without the other party's consent may result in damages and is punishable under the Act if two parties enter into a contract that contains some of each party's personally identifiable information and they expressly or implicitly agree to protect the confidentiality of that information by the terms of the contract.[5] Therefore, we may claim that India has laws in place to monitor and manage data transit via computer networks and the Internet. The Act is ambiguous because there are no established standards or criteria for the protection of people's personal data, nor are there any protocols to help corporations or data fiduciaries.

The Digital Personal Data Protection Act, 2023

After making the required adjustments and amendments to the first plan in response to feedback from the general public, companies, ministers, and the JPC report, the The Ministry of Electronics and Information Technology (MEITy) withdrew the PDP law of 2019 with the purpose of submitting a new law. In November 2022, the MEITy amended the DPDB, 2022 and requested comments from both the general public and business experts which in turn led to the formation of 2023 Act. The previous bill thus underwent the following changes and modifications:

---

[1] *The data boom of the 21st century,* Time of India (Aug. 10, 2023; 05:35 PM), https://timesofindia.indiatimes.com/blogs/voices/the-data-boom-of-the-21st-century/?val=3728&source=app&frmapp=yes.

[2] Information Technology Act, 2000, § 65, No. 21, Acts of Parliament, 2000 (India).

[3] *Who legally authorizes data interception & on what grounds: A study of 5 democracies*, ThePrint (Jan. 30, 2022; 05:11 PM), https://theprint.in/india/who-legally-authorises-data-interception-on-what-grounds-a-study-of-5-democracies/816613/.

[4] Anuradha Bashin v. Union of India, Writ Petition (Civil) No. 1031 of 2019.

[5] Indian Contract Act, 1872, § 19, No. 9, Acts of Parliament, 1872 (India).

- The DPDP Act regulates the handling of digital personal data in India under two circumstances: (i) when this data is obtained from individuals in digital format, or (ii) when it is initially gathered in a non-digital format and afterwards converted into digital form. Therefore, it can be concluded that the DPDP Act is not applicable to the processing of personal data in non-digitized format. The 2023 Act, in contrast to its predecessor, exhibits greater clarity and specificity by excluding 'non-automated' processing and 'offline' data from its scope. Furthermore, the jurisdiction of the legislation has been expanded. The current scope of application of the law has been expanded to include the processing of digital personal data outside of India's jurisdiction, namely in cases where it is related to the provision of products or services to data subjects residing in India. The DPDP Act does not specifically specify whether its provisions are applicable to the processing of personal data pertaining to data principals located outside of India.[1]
- Any offline or online personal data collected in India would be subject to the DPDP law. The measure has also been reinforced to be clearer regarding processing data outside of India if such processing involves selling any goods or creating person profiles.[2]
- The processing of personal data should adhere to legal requirements and necessitate the individual's consent. It is imperative to provide a prior notification prior to soliciting consent. The notice must incorporate comprehensive information regarding the specific personal data that will be gathered, as well as the intended objectives and procedures for processing this data. The act of granting consent can be revoked at any given moment. Consent will not be taken for 'legitimate uses' encompassing the following scenarios: (i) when data has been willingly submitted by an individual for a specific purpose, (ii) when the government provides a benefit or service, (iii) in the case of a medical emergency, and (iv) in the context of employment. Consent for individuals who are under the age of 18 will be obtained from either their parent or legal guardian.[3]
- Before any personal information on a person is collected, they must be informed in advance and given a list of the details that will be requested of them. The person is then free to revoke permission whenever they choose. In the event of a minor, the consent of a natural or appointed guardian is necessary. Situations involving a medical emergency, national security, the welfare of the people, and employment requirements are the only exceptions to this regulation.
- The data principal, referring to an individual whose data is undergoing processing, possesses certain rights, including the ability to: (i) acquire information regarding the processing of their data, (ii) request the correction and deletion of personal data, (iii) designate another individual to exercise these rights in the case of their death or incapacity, and (iv) seek resolution for any grievances. Data principals are entrusted with certain responsibilities. Users are prohibited from engaging in the following actions: (i) submitting a complaint that is fraudulent or lacking in seriousness, and (ii) providing inaccurate information or assuming the identity of another individual in specific circumstances. The failure to fulfil one's obligations will result in a penalty of a maximum of Rs 10,000.[4]
- The data fiduciary, which is the entity responsible for determining the purpose of data processing, is required to fulfil several obligations. Firstly, they must make adequate efforts to ensure the accuracy and completeness of the data. Secondly, they are obligated to establish reasonable security measures to prevent any unauthorised access or breach of the data. In the event of a breach, the data fiduciary must promptly inform both the Data Protection Board of India and the individuals whose data has been affected. Lastly, the data fiduciary is required to delete personal data once the purpose for which it was collected has been fulfilled and there is no longer a legal requirement to retain it (storage limitation). In the context of government institutions, the principles of storage limitation and the data subject's right to erasure are not applicable.[5]
- The new Act mentions the Data Protection Board, as opposed to the previous law, which required the creation of DPAs. Even if the monitoring, reprimanding, and appeals assessment functions are shared by both regulatory bodies, the composition of the Data Protection Board and the process for nomination and removal must be determined by the Union government.
- The law stipulates fines of up to ₹150 crores for failing to meet commitments to minors, and up to ₹250 crores for improper data management leading to violations. However, unlike the previous bill, the current one does not take the turnover of the organizations into account.

Key Principles with regards to the Personal Data

The SPDI Rules provide that collecting organizations are required to disclose specific information to SPDI providers, such as the fact that SPDI is being collected, the reason(s) for such collection, the receivers of the SPDI, and the name and address of the institution collecting and keeping SPDI. Unless the data subject has previously given their approval in the contract under which SPDI was given or the disclosure is required, a person must additionally consent before their information about the data subject is shared with any third party.

Before obtaining the Data Principal's approval, the Data Fiduciary is required by the DPDP Act to give the Data Principal an itemized notice in plain language that lists the personal data it plans to collect and the legal justifications for doing so. When the Data Principal has given her consent to the processing of her personal information prior to the effective date of this Act, the

[1] The Digital Personal Data Protection Act, 2023; § 3, No. 22, Acts of Parliament, 2023 (India).
[2] The Digital Personal Data Protection Act, 2023; § 16, No. 22, Acts of Parliament, 2023 (India).
[3] The Digital Personal Data Protection Act, 2023; § 5, No. 22, Acts of Parliament, 2023 (India).
[4] The Digital Personal Data Protection Act, 2023; § 15. No. 22, Acts of Parliament, 2023 (India).
[5] The Digital Personal Data Protection Act, 2023; § 8. No. 22, Acts of Parliament, 2023 (India).

Data Fiduciary is required to give the Data Principal an itemized notice as soon as is reasonably practical, outlining the personal information the Data Principal has provided to the Data Fiduciary and the purposes for which it has been processed.[1]

Before gathering and spreading SPDI, permission must be obtained in accordance with the SPDI Rules. According to the DPDP Act, an individual is only permitted to use a Data Principal's personal information in accordance with the Rules made public under this Act and for legitimate purposes to which the Data Principal has consented or is assumed to have consented in accordance with its requirements. Furthermore, it defines a legitimate aim as any goal that is not expressly forbidden by the law.

The DPDP Act lays forth few guidelines for how collecting organizations should handle personal data. These include consent provided in line with the 'deemed consent' provision to treat a medical emergency, for professional reasons such as combating corporate espionage, safeguarding the confidentiality of trade secrets, and for a data principal. They also encompass authorization issued for hiring, dismissing, providing any service or benefit requested by an employee who holds the position of Data Principal, confirming attendance, and rating performance. The DPDP Act constrained data processing to be done only for legitimate purposes in accordance with the aforementioned criteria.

According to the SPDI Rules, SDPI may not be kept around any longer than is needed by any other applicable laws or for the reasons for which it may be properly utilized. The DPDP Act states that if a data principle withdraws her consent, the data processors must stop processing personal data or be compelled to stop within a reasonable length of time. Data Fiduciaries are not allowed to keep any private data in this circumstance.

Although the DPDP Act seeks to guarantee that whoever chooses the purpose and strategy for processing personal data is responsible for doing so in a fair and reasonable way, neither the IT Act nor the SPDI Rules explicitly state this principle. Every data fiduciary and data processor are required under the DPDP Act to safeguard any personal data they own or manage by putting in place the essential security precautions to avoid a personal data breach. According to the DPDP Act, a Data Fiduciary must abide by the requirements for any processing carried out on their behalf or for the benefit of consumers. In the case of a personal data breach, the Data Fiduciary or Data Processor should promptly notify the Board and any impacted Data Principal (to whom any affected personal data belongs). A variety of new general responsibilities for data fiduciaries are mentioned in the proposed DPDP Act, along with specific obligations to protect children's personal data with care.[2]

The SDPI Rules provide that data owners must give their consent before their SPDI can be transferred. However, there is not a specific provision that permits transfers abroad. The RBI has announced regulations that mandate enterprises preserve consumer data when contracting out financial services. Sector-specific restrictions may apply to data transmission. According to the DPDP Act, the Central Government may, subject to any norms and criteria that may be created, notify any countries or territories outside of India to whom a Data Fiduciary may transmit Personal Data.

The Rules must take a firmer stance regarding the permission procedure in the instance of a cross-border data transfer rather than using the customary method of getting approval from the data subjects. Given India's low level of digital literacy, it can be difficult to obtain the true agreement of those who are unaware of the circumstances, objective, and nature of the information being requested. Explicit consent must be acquired, and extra consent must be required if the data is moved outside of India, according to the standards. The terms and conditions and other important information pertaining to the data transfer must be made available to the data subject in text-to-speech format in their preferred language. Consciously providing the consent, such as by checking the consent box, is required.

Criticisms of DPDP Act 2023

Although the DPDP Act has received commendation for its effectiveness as a comprehensive data protection framework, it is important to acknowledge that there are certain drawbacks that should not be overlooked. There are concerns over the fact that several sections of the DPDP Act are still contingent upon determinations made by the Central Government. This particular element gives rise to legitimate worries regarding the possibility of unregulated and capricious rule establishment, which may result in uncertainty and potential deficiencies within the regulatory structure. Moreover, it is noteworthy that the DPDP Act, which aims to safeguard the rights of data principals, paradoxically puts obligations on these individuals.[3]

Like the 2022 Bill, the DPDP Act also has the capacity to grant exemptions to the Central Government. Nevertheless, in this particular version, these exemptions have been further extended, hence prolonging the lack of substantial requirements to mitigate excessive surveillance practises. The Central Government also possesses the authority to grant exemptions to certain fiduciaries or categories of data fiduciaries from certain rules, with a specific focus on start-ups. According to the Act, the term "startup" is defined as a privately held company, partnership firm, or limited liability partnership that is incorporated in India and meets the eligibility criteria and recognition process established by the department responsible for startups within the Central Government.

Through its presumed consent clause, the 2022 Bill permitted the Central Government to presume the consent of data principals in certain circumstances, without allowing them to opt out. The DPDP Act preserved this provision while redesigning it to be termed as "certain legitimate uses."[4]

---

[1] Aishani Singh, *India: Brief Note on SPDI*, Mondaq (Jun. 25, 2020), https://www.mondaq.com/india/privacy-protection/956252/brief-note-on-spdi.
[2] *Ibid.*
[3] Vatsal Gaur, *India: A Dawn Of A New Era For Data Protection In India: An In-depth Analysis Of The Digital Personal Data Protection Act, 2023*, *Mondaq* (Aug. 15, 2023), https://www.mondaq.com/india/data-protection/1355250/a-dawn-of-a-new-era-for-data-protection-in-india-an-in-depth-analysis-of-the-digital-personal-data-protection-act-2023- .
[4] *Ibid.*

The implementation of a transition period is crucial in order to ensure a seamless adjustment for enterprises. The DPDP Act imposes novel and rigorous responsibilities that may necessitate substantial adaptations from data fiduciaries. The absence of a transition phase during the implementation of the DPDP Act may result in a significant prevalence of non-compliance. By allowing businesses a sufficient transition period, they are given the necessary time to align their operations and comply with the requirements of the DPDP Act. This helps to minimise any disruptions and ensures a smooth transfer to the new data protection landscape.

Current Scenario with regards to Data Protection

An all-time high and an increase of over 28% from 2020, the research states that the average value of a data breach was ₹17.9 crore in 2023. In India, phishing attempts accounted for around 22% of all attacks, while compromised or stolen credentials accounted for 16%. The second most costly root cause of breaches was malicious insider threats, which cost close to ₹18.8 crore and amounted to ₹19.1 crore.[1]

Detection and escalation expenses, which make up the majority of breach costs, increased 45 percent within the same time period, indicating a shift toward more thorough breach investigations. Information from different contexts (public cloud, private cloud, on-premise) was lost in 28% of the data breaches in India that were investigated. This shows that attackers were effective in sneaking into a number of scenarios. The most notable impact of automation and artificial intelligence on the firms under examination was the speed of breach identification and control.[2]

Conclusion and The Way Forward

Given the lack of a comprehensive law to handle the issues connected to data privacy, India's condition with regard to data protection was grave. Despite the existence of the Indian Law of Contract and the IT Act, both laws had little to do with data privacy hence with the coming of DPDP Act 2023 the dire need for a uniform law is no more now.

By passing the required legislation to preserve people's privacy and the security of their personal information, as well as to punish violators, the state has a duty to protect society. As a consequence, the PDP bill of 2019 was presented in the parliament before being pulled in response to complaints. Once the required changes to the prior legislation had been completed, the DPDP Act of 2023 was then presented. But despite everything they did, not a single law was approved until now.

The DPDP Act represents a unique strategy employed by India in order to protect personal data, signifying the result of comprehensive deliberations subsequent to its initial proposal. The enactment of this data protection legislation signifies a significant milestone in the protection of individuals' personal data, as it addresses long-standing need in light of the growing number of internet users, the proliferation of data, and the expansion of cross-border trade.

The DPDP Act, in its totality, represents India's distinctive position on contemporary data protection, which has been enhanced through comprehensive dialogues conducted after the drafting process. Although the terms of the Indian data protection law are not as comprehensive as those of regulations such as the General Data Protection Regulation (GDPR), it requires a substantial change in the manner in which Indian enterprises address privacy and personal data.

Nevertheless, the DPDP Act is not impervious to criticism. There are differing viewpoints on the potential impact of this policy on innovation and privacy. Critics claim that the apparent strictness of the policy could impede innovation. On the other hand, proponents argue that the policy may not provide sufficient safeguards for individual privacy, particularly in light of the discretionary powers allowed to the Central Government in relation to personal data processing. The impending regulations implemented via delegated legislation will have a significant impact on shaping these particular facets. The implementation of a standardised procedure for the publishing of regulations, along with the inclusion of industry consultations, as exemplified by the revisions made to the Information Technology Rules pertaining to online gambling, would provide a strong framework for data protection that would have positive implications for the whole technology sector in India.

[1] *Average cost of data breach in India touches high of Rs 17.9cr in 2023*, Economic Times (Jul. 26, 2023; 08:29 AM), https://telecom.economictimes.indiatimes.com/news/enterprise-services/average-cost-of-data-breach-in-india-touches-high-of-rs-17-9-cr-in-2023-ibm-study/102122064.

[2] *Ibid.*