

---

# DATA PROTECTION IN INDIA: FROM PAST TO PRESENT, MAPPING THE EVOLUTION OF PRIVACY LAWS

---

Shivalika, LL.M., SRM University, Faculty of Law, Sonapat, Haryana

## ABSTRACT

This research paper tends to discuss the evolution of India's data protection laws. Through this research paper I have tried to trace the development of data protection laws, analyzing key milestones and shifts in regulatory frameworks. Beginning with an overview of early privacy concerns and legislative initiatives, we delve into the landmark moments that have shaped India's approach to data protection. Through this historical lens, we highlight the progression towards more comprehensive and robust privacy regulations, such as the introduction of the Personal Data Protection Bill from its nascent stages and then finally enactment of the DPDP Act, 2023 which is the byproduct of different drafts and consultations.<sup>1</sup> By mapping this evolution, I have aimed to provide insight into the trajectory of data protection in India and its implications for individuals, businesses, and society as a whole.

---

<sup>1</sup> Ms. Shiva Kanwar, Mr. Mayank Manish, "Evolution of India's Data Protection Law: A Primer" *ICRIER* 1 (2023).

## INTRODUCTION:

***Data protection is not about protecting data; it's about protecting people***"- Marc Rotenberg, President and Executive Director of the Electronic Privacy Information Centre (EPIC), Washington, D.C

As correctly said by Sir Marc Rotenberg, this statement is fundamental in the current era which is exponentially moving towards digitization and data-driven processes. The basic needs of humans in this 21st century have totally transformed and now the entire world is discussing the capability of data- which people now call "gold mine".<sup>2</sup> Around 328.77 million terabytes of data are created each day which includes data that is newly generated, copied, captured and consumed. It makes us understand that data is not just an abstract information but it represents an individual's personal lives, identities and personal details. Clive Humby, a British Mathematician declared "*data as the new oil*" in 2006 with the only exception that unlike oil, data can be used and reused.<sup>3</sup>

Right to privacy is one of the most fundamental and basic rights which has been recognized by various countries. Many countries, including India, guarantee this right as part of their fundamental rights in the Constitution. Any encroachment or breach of the right to privacy of others can lead to legal consequences. Right to privacy can be defined as the right which protects the inner realm of the individuals from any interference from State or even non- State components and allows individuals to make decisions. Although the right to privacy can include physical privacy, with the advent of the internet, the concept is now more about digital privacy and data protection.

Digital privacy or Data Privacy is often defined as the level of privacy of an individual regarding his/her personal information in the digital world. Many users at the digital platforms don't realise that their identities, internet history and data are continuously being monitored, managed, processed and even stored by these digital platforms. Thus, for ensuring maximum security and to avoid the misuse of the same, certain compliances must be met. Data protection refers to the practice of safeguarding information from any unauthorised access, disclosure, alteration or destruction. Data Protection regulations govern the collection, transmission and

---

<sup>2</sup> HT Correspondent, "Data protection Act will safeguard future generations, says PM", The Hindustan Times, 11th February 2024.

<sup>3</sup> What Lies beneath the PR Blitz On the New Data Protection Act, <https://thewire.in/government/what-lies-beneath-the-pr-blitz-on-the-new-data-protection-act> (last visited November 27, 2023).

usage of data which involves various measures to ensure security and privacy of data. Here, data can include personal details and information, business information, financial records and more.

**Data protection encompasses the following:**

1. **Data Security:** Implementing technical and organisational measures and safeguards to prevent data breaches.
2. **Privacy Protection:** To protect an individual's personal, business or financial information adhering to legal and regulatory norms.
3. **Data Backup and Recovery:** Storing data and creating copies to ensure it can be restored in case of data loss or corruption.
4. **Access Control:** Restricting access of data to any unauthorised user.
5. **Data Monitoring and Auditing:** Tracking data usage and changes to detect and respond to any suspicious activities.

**RELEVANCE AND SIGNIFICANCE OF THE RESEARCH:**

In the present digital era, it is very important to understand how data protection and privacy laws have changed over time in India. This is necessary because technology has grown so fast and personal information has become digitized, leading to urgent calls for people's privacy rights and responsible management of information.

Several stakeholder groups find this research relevant:

- **Policy Makers and Regulators:** Policymakers would benefit from knowing about the past development of data protection law in order to design future policies. Knowledge from previous successes and failures can help policy makers draft efficient and forward-looking legislation that consider issues on privacy while promoting economic growth through innovation.
- **Businesses and Organizations:** There is a need for companies operating in India to comply with data protection regulations not only as a way of avoiding legal processes

but also as a method of ensuring customer confidence. By knowing how privacy regulations have changed over time, firms can change their ways of doing things based on current standards which makes them more reputable or competitive within their sectors.

- **Legal Professionals and Scholars:** Comprehensive understanding of the historical evolution of privacy regulations in India serve as a valuable resource for legal analysis, case studies and academic discussions on privacy rights, data protection and regulatory frameworks.
- **Civil Society and Advocacy Groups:** Civil society organizations and advocacy groups play a crucial role in promoting privacy rights and holding governments and corporations accountable for data protection practices. By tracing the evolution of privacy laws, these groups can identify gaps, advocate for stronger protections, and empower individuals to assert their privacy rights.
- **Individuals:** As individuals increasingly navigate an interconnected digital world, understanding their rights and protections concerning personal data is vital. This research can empower individuals to make informed choices about their online activities, demand accountability from service providers, and advocate for stronger privacy safeguards.

## REVIEW OF LITERATURE:

- **Articles 14, 16, 19 and 21 of the Indian Constitution:**<sup>4</sup>

These articles of the Indian Constitution talk about various fundamental rights given to the citizens of India. It gives insights on how digital privacy became a part of Article 21 that is “Right to life”.

- **Digital Personal Data Protection Act:**<sup>5</sup>

The DPDP Act has been enforced in 2023 in India which has now enlarged the scope of data

---

<sup>4</sup> The Constitution of India, arts. 14,16, 19, 21.

<sup>5</sup> The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

protection and digital privacy by including data fiduciaries and data principals in the Act.

- **The Information Technology Act:<sup>6</sup>**

The Information Technology Act, 2000 is an act to provide legal recognition for transactions which have been carried out through electronic mode. It gave legal recognition to electronic records and digital signatures and the formulation of the Controller of Certifying authorities to regulate the issuance of digital signatures. This act will be referred to earlier as the DPDP Act, it was the only act in India which dealt with the digital domains and included penalties and punishments in case of breach.

- **The Aadhar Card Act:<sup>7</sup>**

The Aadhar Card Act was enacted to establish and facilitate a unique identification system for residents of India. This unique identification system involved a 12-digit identification number called Aadhaar. This act explains how core biometric information is taken from the citizens which is the part of digital privacy and its protection provisions followed.

- **Landmark case of *K.S. Puttaswamy v. Union of India*:<sup>8</sup>**

The landmark case, gave an insight as to how digital privacy and data protection laws came into existence and how it led to the constitution of the SriKrishna Committee. This is the primary focal point of data privacy and data protection laws in India.

## **RESEARCH OBJECTIVE:**

To trace the evolution of data protection law in India

## **RESEARCH QUESTION:**

How have the data protection and data privacy laws evolved in India?

## **RESEARCH METHODOLOGY:**

The research will primarily involve a **doctrinal research approach** which will include an in-

---

<sup>6</sup> The Information Technology Act, 2000 (Act 21 of 2000).

<sup>7</sup> The Aadhar Card Act, 2016.

<sup>8</sup> K.S. Puttaswamy v. Union of India AIR 2017 SC 416.

depth examination of legislative texts of the statutes, official government documents, and academic literature pertaining to data protection and data privacy in the digital domain in India and utilisation of secondary sources such as case laws, articles and expert opinions to supplement understanding.

## **THE BIRTH OF LEGAL SAFEGUARDS: EARLY RECOGNITION OF PRIVACY CONCERNS:**

Our country India is special because of being full of diversity. The kind of information and data we generate is humongous. If someone were to look at the data of our railway passengers, it would only become a subject of huge research for the whole world.<sup>9</sup>

The DPDP Act is the first cross-sectoral law on personal data protection and has been enacted after having more than half a decade of deliberations.<sup>10</sup>

### **Timeline: The road map to the DPDP ACT:**

#### **2010:**

- India's journey towards a comprehensive data protection law began.<sup>11</sup>

#### **2012:**

- Justice A. P. Shah Committee

Issued nine national privacy principles and recommended the creation of an overarching law for privacy protection that were: Notice, Choice and Consent, Collection Limitation, Purpose Limitation, Access and Correction, Disclosure of Information, Security, Openness and Accountability.

#### **2017:**

- Right to privacy was declared as a fundamental right under Article 21 of the

---

<sup>9</sup> *Supra* note 2 at 2.

<sup>10</sup> Anirudh Burman, "Understanding India's New Data Protection Law", Carnegie India 1 (2023).

<sup>11</sup> Evolution of Data Protection in India; Detailed Analysis, available at: <https://www.legalserviceindia.com/legal/article-14487-evolution-of-data-protection-in-india-detailed-analysis.html#:~:text=In%202022%2C%20A%20new%20Draft,assent%20on%20Aug%2011%2C%202023.> (Last visited April 7, 2024).

Constitution by the Supreme Court of India in *K.S. Puttaswamy v. Union of India*<sup>12</sup>

- Advised Central Government to establish a data protection policy that balances the needs of individuals
- Justice Srikrishna Committee was formed to examine the issues relating to data privacy and to recommend possible solutions.

**2018:**

- The report given by the Justice Srikrishna Committee (2018 Report titled *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*) along with a draft Personal Data Protection Bill 2018 to the Ministry of Electronics and Information Technology in July 2018.

**2019:**

- Personal Data Protection (PDP) Bill, 2019 was introduced in Lok Sabha
- Joint Parliamentary Committee was formed to study and consider the Bill

**2021:**

- Joint Parliamentary Committee Report

Report contained a list of policy recommendations and a draft bill titled the Data Protection Bill, 2021.

**2022:**

- August: Withdrawal of PDP Bill, 2019 from parliament
- November: Draft Digital Personal Data Protection Bill, 2022 was released for public consultation.

---

<sup>12</sup> Supra note 8 at 5.

**2023:**

- Digital Personal Data Protection Act, 2023<sup>13</sup> was enacted and passed by both houses of Parliament and received assent of the President.<sup>14</sup>

## **THE LANDMARK JUDGEMENT<sup>15</sup>**

The Supreme Court reaffirmed the right to privacy as a fundamental right under Article 21 of Part III of the Indian Constitution for the citizens of India in 2017.<sup>16</sup> The judgement did not prescribe any mechanism through which this right is to be protected.<sup>17</sup> However, the judgement also held that the right to privacy is not an absolute right and depends upon three conditions that are: legality, legitimate aim and proportionality.<sup>18</sup>

## **THE DATA PROTECTION BILL, 2019**

- The bill talked about personal data (like passwords, health information, financial information, official identification, information about one's sexual life, sexual orientation, biometric and genetic information, and information revealing caste, tribe, religious or political affiliations etc.) sharing on consent of the individual and placed duties and obligations on data fiduciaries (an entity which processes data like natural and artificial persons, government etc).
- The bill also talked about a right: “Right to be forgotten” which gives power to users/ individuals to remove, restrict, delink or amend any information online which may be inaccurate, humiliating or incorrect.
- The constitution of an independent regulatory body was also suggested that was Data Protection Authority (DPA) to do the following functions:
  - a. Enforcement and monitoring of personal data protection laws in India

---

<sup>13</sup> *Supra* note 5 at 4.

<sup>14</sup> Ms. Shiva Kanwar, Mr. Mayank Manish, “Evolution of India’s Data Protection Law: A Primer” *ICRIER* 1 (2023).

<sup>15</sup> *Supra* note 8 at 5.

<sup>16</sup> HT Correspondent, “Data protection Act will safeguard future generations, says PM”, *The Hindustan Times*, 11th February 2024.

<sup>17</sup> *Supra* note 10 at 6.

<sup>18</sup> *Supra* note 14 at 7.



- b. Setting standards for the legal policies and affairs
  - c. Spreading awareness
  - d. Conducting research on evolving technology
  - e. Handling any grievances and setting up inquiry and adjudication. However, the order of DPA is subject to appeal
- Obligations on Fiduciaries under this Bill:
  - a. Data can only be stored and used for clear, specific and lawful purposes
  - b. To ensure user safety through openness
  - c. To conduct data protection impact assessment before introducing new technologies in the market
- The Bill made it very clear to include data processors who are not physically present in India in the category of data fiduciaries.
- Exceptions: public welfare, law, and order, employment, emergency situation, where an individual is not in the stage of providing consent to the state, security of state, legal proceedings and research and journalistic purpose.
- The committee has shown greater interest in the protection of data of children as it prohibits companies from doing activities like monitoring and tracking any child's activity and restricts any targeted advertising which is not in the interest of the child.

The government of India made few revisions to address the shortcomings in this draft bill and introduced personal data protection. Bill 2019, which helps to establish a framework for organisational and technical measures in data processing, It lays down standards for social media, intermediaries, cross-border transfers, accountability of entities, processing, personal data and remedies for harmful processing which built the trust between individuals and entities processing the personal data and further protected data .This bill not only targeted technology, e-commerce and social media firms but also targeted real estate, healthcare and pharmaceutical industries.

**PERSONAL DATA PROTECTION BILL, 2019**

The Bill seeks to mimic provisions of Information Technology Act, 2000 (Section 43-A) which pertains to the compensation that businesses are required to pay for any breach of data privacy and any security breaches.

- **Objectives:**

- a. The right to privacy is a fundamental right and this bill focused on protection of this fundamental right as it protects personal data of every individual
- b. The importance of establishing a collective culture was laid down which supports a free and equitable digital economy while protecting individuals' right to privacy.

- **According to the Bill:**

- a. Before processing any data, data fiduciaries and processors must take the consent of the user/ individual

Exceptions to the consent: for court-mandated compliance, for law enforcement, public benefit, service or medical emergency

- b. Duties of Data fiduciaries and Data processors:

The Data Fiduciary should notify data principals for collecting data, should seek consent for processing of data, should collect evidence and store the data only when notice is served, should allow consumers to withdraw their consent as and when required and also correct or erase their data and also transfer their data

- c. Division of Data according to this Bill:

- Personal data v. non-personal data: Data which is related to characteristics, traits or attributes which helps to identify an individual is called personal data. Non-personal data is the aggregated data that is unable to identify a specific person is called non-personal data.

- Personal data is classified into two types: Sensitive Data and Non-Sensitive Data where personal data comes under the category of Sensitive Data
- d. The bill granted the DPA authority to impose fines on any company that violates the provisions established by the government or the DPA. The maximum penalty as mentioned in the bill is 150 million Indian rupee or 4 % of the respected companies' global turnover for the previous financial year.

- **Major criticisms on this Bill:**

Section 35 of the Bill gives supreme power to the government to process the data without consent of the user in case of “necessary or expedient” in the “interests of sovereignty and integrity of India, national security, friendly relations with foreign states and public order.”

The Personal Data Protection Bill, 2019 was withdrawn by the Central government in 2021 because the Joint Committee of Parliament (JCP) suggested 81 amendments and 12 recommendations. In 2022, the Central government after taking JCP's recommendations into consideration, decided to withdraw and brought a new bill with a more comprehensive legal framework that was: Digital Personal Data protection Bill, 2022 was released for public consultations but feedback of the public was not made public. In 2023, the Indian government introduced the Digital Data Protection Bill and this Bill was enacted as the DPDP Act, 2023 which received the president's assent on August 11, 2023.<sup>19</sup>

## **EMPOWERING INDIVIDUALS: RIGHTS AND PROTECTION UNDER THE DPDP ACT:**

The Digital Personal Data Protection Act, 2023 (DPDP Act) has been a significant milestone in India's legal journey towards safeguarding individual privacy in the digital era.<sup>20</sup> The DPDP Act, 2023 provides a framework for protecting individuals' personal data in the last parliamentary speech before the elections, the Prime Minister of India, Narendra Modi said

---

<sup>19</sup> *Supra* note 11 at 6.

<sup>20</sup> *Ibid.*

that “Data Protection Act will safeguard future generations.”<sup>21</sup>

### UNDERSTANDING FEW TERMS:

	DATA PRINCIPAL	DATA FIDUCIARY	SIGNIFICANT DATA FIDUCIARY
Meaning	Persons or legal guardians/ parents of minor or persons with disabilities	Person, business or other organization that processes data	Significant Data Fiduciaries are data fiduciaries with additional obligations
Rights/ Obligations	<ul style="list-style-type: none"> <li>a. Right to information about their personal data</li> <li>b. Right to get information incase any personal data is shared</li> <li>c. Right to correct and erase, complete or update the personal data</li> <li>d. Right for grievance redressal incase of any grievance</li> <li>e. Right to nominate</li> </ul>	The Act requires data fiduciaries to protect the personal information which is under their control by putting in place “reasonable security and measures”. The data fiduciary also has to notify the Board incase of a data breach.	<ul style="list-style-type: none"> <li>a. Designating an Indian-based data protection officer</li> <li>b. Hiring a data auditor to assess compliances</li> <li>c. Performing impact analysis on data security</li> <li>d. Going through and checking regular compliance audits</li> </ul> <p>Penalties for breach: can go up to INR 250 crore</p>

<sup>21</sup> HT Correspondent, “Data protection Act will safeguard future generations, says PM”, The Hindustan Times, 11th February 2024.

**ANALYSIS OF THE DPDP ACT:**

- **Governs two types of data:**

- a. Data which is collected from Data Principals in digital format.
- b. Data which is collected initially in non-digital format and later converted into digital format.

- **Covers extraterritorial digital personal data:**

Personal data which is outside India in digital format is covered under this act as long as it is related to providing of goods or services to data principals based there.

- **Processing of Personal Data:**

The Act defined the word “processing” in its definition clause as a whole or partially automated operation or a series of operations which are conducted on digital personal data. These operations cover a wide range of activities like gathering, logging, structuring, organizing, storing, modifying, using, aligning, combining, limiting, deleting, destroying, sharing and disclosing data. The processing must be done only for lawful purposes.<sup>22</sup> Consent given by the person whose data is being processed for specified purpose must be “free, informed, specific, unambiguous and unconditional with an affirmative action”. A clear notice must be provided to consumers containing details like the rights of such person giving consent and the grievance redressal mechanism and individuals can withdraw such consent at any time.<sup>23</sup>

- **Processing of Children’s Data:**

The DPDP Act does not define “verifiable” consent specifically. The act does not seek any parental approval that may be verified. If the processing is deemed safe then the Central Government may reduce the age at which parental consent is deemed to be required. The data fiduciaries have also been refraining from handling any personal information that seems to be harmful to a child’s well-being.

---

<sup>22</sup> *Supra* note 10 at 6.

<sup>23</sup> *Ibid.*

- **Exemptions From Obligations Under the Law:**

- a. Where processing is necessary for enforcing any legal right or claim
- b. Personal data has to be processed by courts or tribunals, or for the prevention, detection, investigation, or prosecution of any offences
- c. Where the personal data of non-Indian residents is being processed within India
- d. Where processing is done in the interests of sovereignty and integrity, security of India, friendly relations with foreign states, maintenance of public order or preventing incitement of any cognizable offence.
- e. Data processing if needed necessary for research, archiving or statistical purposes
- f. Government can exempt certain classes of data fiduciaries from some provisions<sup>24</sup>

## CONCERNS REGARDING THE DPDP ACT:

This chapter will also scrutinise the Act's adaptability to rapid technological advancements such as artificial intelligence, biometrics and advanced data analytics, and whether the act's current provisions address the complexities of these innovations.

- **Concept of Delegated Legislation:**

In the concept of delegated legislation, various administrative agencies established by law capable of exercising power, administers and governs on behalf of the government. In this act, excessive reliance on delegated legislation can be seen which has the potential to excessive use or abuse of power. In the dissenting judgement in the verdict of the Supreme Court on demonetisation, it was stated by Justice B.V. Nagarathna that "*unguided and unlimited powers under delegation would be ex-facie arbitrary*". The Act is filled with one phrase "*as may be prescribed*" raises so many unanswered questions which raises concerns about the lack of clarity and specificity.

- **"Legitimate uses" do not require consent:**

---

<sup>24</sup> *Supra* note 10 at 6.

The term “legitimate uses” has been used in the Act to wither away the responsibility of data fiduciary of taking consent from the user in several cases. *“The scope of this term is very expansive and thus leaves with very little of the term’s purview”*

Personal information made publicly available by any person or data principle to comply with any law is excluded from the purview of the act. One such instance is of Clearview AI, a facial recognition company in the United States who was using publicly available social media photographs of people to train their AI and even for identifying people.

- **The Right to Information of citizens of India:**

The DPDP Act<sup>25</sup> provides for “non-disclosure of all personal information to the citizens for example official information, such as minutes of a particular meeting.”

- **Exemptions from taking parental consent:**

In making an attempt to protect children, every single website and every single app will have to verify the age of every individual using that service. Section 9(4)<sup>26</sup> The Act allows the government to declare any class of Data Fiduciaries which can be exempted from the restrictions in possessing children’s personal data. Section 9(5)<sup>27</sup> The Act permits the government to exempt any Data Fiduciary from the need of seeking parental consent for processing personal data. The Data Fiduciary can also track or monitor the behaviours of children which raises concerns of potential tracking and targeted advertising without their knowledge.

- **Striking an Inharmonious Chord:**

The DPDP Act permits the Union Government to appoint the chairperson and board members, without specifying selection procedure. This provision contradicts with the recommendations of the Joint Parliamentary Committee which sought the nomination of board members by the Selection Committee composed of the Attorney General of India, Independent expert from fields such as data protection, information technology or cyber laws and directors.

---

<sup>25</sup> *Ibid.*

<sup>26</sup> Digital Personal Data Protection Act, 2023 (Act 22 of 2023), S. 9 (4).

<sup>27</sup> Digital Personal Data Protection Act, 2023 (Act 22 of 2023), S. 9 (5).

- **Voluntary undertaking:**

Section 32<sup>28</sup> of the DPDP Act, introduces “Voluntary Undertaking” from those in non-compliance with the Act’s provision and to stop further enquiry.

- **Evasion of compensation and accountability:**

There is absence of provision for awarding compensation by the Data Protection Board to aggrieved data principals under Section 34<sup>29</sup>. This deficiency can result in hampering the effectiveness of the legislation.

- **A realm of exemptions and accountability erosion:**

Section 17<sup>30</sup> grants the Union government the power to exempt government agencies and data fiduciaries in the name of interests of sovereignty and integrity of India, security of the State, friendly relations with other States, maintaining public order. This can result in undue infringement of personal data privacy rights and evasion of responsibilities of government.

- **A range of ambiguities and omissions:**

The act introduces ambiguity and omissions in critical areas like data portability, data storage requirements, processing of physical or non-digital personal data. It opens gateways to different interpretations and potential misuses of the legislation.

- **Employer’s power over employee’s personal data:**

Section 7(i)<sup>31</sup> states that employers are with the authority to access and store personal data for employment-related purposes which can potentially raise privacy concerns in the minds of employees.

- **Exclusion of physical or non-digital data:**

The act does not pay any heed to non-digital or physical personal data raises questions on the comprehensiveness of the current legislation which contradicts the recommendations of the

---

<sup>28</sup> Digital Personal Data Protection Act, 2023 (Act 22 of 2023), S. 32.

<sup>29</sup> Digital Personal Data Protection Act, 2023 (Act 22 of 2023), S. 34.

<sup>30</sup> Digital Personal Data Protection Act, 2023 (Act 22 of 2023), S. 17.

<sup>31</sup> Digital Personal Data Protection Act, 2023 (Act 22 of 2023), S. 7(i).



Joint Parliamentary Committee on previous Bill, 2019 and overlook potential privacy risks.

- **Exclusion or limited laws relating to Artificial Intelligence:**

The act does not provide specific guidelines on Artificial Intelligence and its implications in the digital era. With the advancement of technology in the field of AI, stringent laws are required to cover its various aspects like legal liability, copyright or ownership issues which are not covered by the DPDP Act.

## **CONCLUSION:**

The Digital Personal Data Protection Act (DPDP Act) of 2023 undoubtedly marks as a crucial step in India's journey of protecting digital privacy of individuals.

This Act may not be flawless or extensive in use; it does considerably protect the data of Indian citizens as it sets clear laws on how the information will be governed. The act gives power to the users/ individuals to decide what happens to their data and puts the data fiduciaries on their toes, knowing they are accountable for any unethical information handling. This power play increases the transparency in the information world and strengthens the integrity benefitting both the individuals and institutions. It promotes innovation and thus fosters economic growth.

Overall, the Act will regulate and balance conflicting interests between individual's privacy and digital innovations in the country, and that will create the possibility of the overall protection of consumers' rights and data. For these reasons, the passing of the Act can be evaluated as a positive development for India's digital future. However, it is important that the implementation and the enforcement of the Act are robust. Additionally, there is room for further development in terms of restricting the use of consumer data by the state. Moreover, it is possible that changes can happen and the law has to be adjusted to reflect the changes.<sup>32</sup>

---

<sup>32</sup> *Supra* note 11 at 6.