IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# Data becomes a product- Analysing with respect to the New Digital Personal Data Protection Act, 2023

**MANAS RAJDEEP**

Student of Law

AMITY UNIVERSITY, LUCKNOW

Introduction and Background

With more than 760 million active internet users India is the Second-largest make in the world. In a 2017 ruling, the Supreme Court of India recognized the right to privacy, and in August 2023, the Indian parliament passed a comprehensive data protection law, the Digital Personal Data Protection Act (DPDP).

During August 2023, the parliament of India approved the Digital Personal Data Protection act 2023. This new law. The new law was passed after more than five years of debate and is the first multi-disciplinary personal data protection law in India.

The main question is whether the law enacted after such long period resulted in a GOOD LAW, does this law can protect the personal data.

The Data Protection Act 2023 is the second version of the bill, which was introduced in the parliament, but overall, it is the fourth one. All these four drafts were preceded by a landmark judgement by India's Supreme Court in **Justice K.S Puttaswamy and Anr. V. Union of India and ors.**

## Judgement

Right to privacy is a part of right. But the judgement does not establish procedure for ensuring the protection of the right to informational privacy, nor did it define the precise parameters of that right.

## Key Features of Data Personal Data Protection Act 2023

When we compare the new Act with the previous bills introduced in 2019, the DPDP act, 2023 is more modest- It offers less consumer protections and business duties. The regulatory framework is less complicated, but it also gives the federal government certain unrestrained discretionary powers in particular situations.

When "data becomes a product," it usually refers to how companies are making money off people's personal information. The idea is gathering, processing, selling, or otherwise utilizing personal data for a range of uses, including product creation, analytics, and targeted advertising.

The handling of personal data by corporations may change if a new Digital Personal Data Protection Act is enacted in 2023. Based on typical components of data protection regulations, the following is a broad analysis:

- Agreement and Openness:

The necessity of getting people's explicit and informed consent before collecting and using their personal data may be emphasized by the Act. Companies may be forced to disclose to consumers the reasons for data acquisition and the intended uses of their personal information.

- Minimizing Data and Restricting Use:

Businesses may be encouraged by the Act to gather just the information required for the intended use. Businesses may be forced to restrict data use to the reasons for which it was initially gathered.

- Rights of Users:

People may be given rights over their personal data, such as the ability to see, edit, remove, or transfer their data to other services. The Act may specify how users can exercise their rights and require companies to make these rights easier for consumers to use.

- Security Procedures:

Businesses may be required to put in place sufficient security measures to guard against unauthorized access, disclosure, modification, and destruction of personal data.

- Notification of information security breaches:

The law may require organizations to immediately report information security breaches and ensure that they are notified to relevant persons and authorities. Reporting and Management, Companies may be required to implement internal policies and procedures to ensure compliance with the law showing responsibility for the processing of personal Data,

- Enforcement and Sanctions

the Act may impose sanctions for non-compliance, giving regulatory authorities the power to enforce compliance and punish organizations that breach data protection principles.

As data becomes a product, a strong data protection framework can influence how companies process personal data. They can be more careful about obtaining consent, ensuring data security, and respecting users' rights, which can affect the way they monetize and use personal data. It could also promote a more ethical and transparent approach to data business practices.

## How DPDP Act protects the privacy, does it really safeguard the privacy?

The Act of 2023 creates a data protection law for the first time in India. It requires consent before processing personal data and contains a limited number of exceptions that are clearly listed in the law. It offers consumers the right to access, correct, update, and delete their data in addition to the right to name. This creates additional safeguards for the processing of children's data. For companies, it sets limits on the purposes of use and obligations to inform about the collection and processing of data and obliges them to implement security measures. The law requires companies to set up complaint's mechanisms. The DPB also handles appeals and complaints and has the power to impose penalties for violations of the law.

Thus, for the first time in India, there is a mandatory data protection framework. The existence of the law will gradually lead to a minimum level of behaviour and compliance by companies that collect data. In this regard, a critical variable will be the government's approach to implementing and enforcing the law - for example, whether enforcement targets data-intensive companies or the economy would be an important factor.

Restrictions and obligations to organization that process personal data.

1. Take consent from individual before the organization process their personal data. The organization must inform the individual before processing their personal data unless an exemption applies.
2. The data can be used only for the purpose it is obtained for unless they have taken the consent of the individual for any other use.

3. The organization is responsible to protect the data of the individual from any unauthorized access, use, disclosure.

In addition to the above responsibilities, data processing organizations can take the following steps to better prepare for compliance:

Assess data processing operations: Organizations should assess their data processing operations to identify areas where they may need changes to comply with the DPDP Act. Development of a data protection policy: Organizations must develop a data protection policy that defines their responsibility to protect personal data and describes data handling practices. Appoint a data protection officer or data protection officer: organizations that process personal data on a large scale must appoint a data protection officer. The Data Protection Officer is responsible for ensuring that the organization complies with the DPDP Act. Appoint an independent auditor to conduct periodic audits to ensure continued compliance.

Cross-selling is one of the most popular strategies. Digital payment platforms like UPI or PPI (e-wallet) providers are a cash-burning business. Platforms share huge cashbacks, incentives to acquire and maintain an active user base. So, you create a payment company that acts as a data mine. You collect a large amount of information about your users and merchants. Then use this information to cross-sell other more profitable products. Like debts, capitals, and insurance. Your entire payment business is a "customer acquisition cost" for another company - another product. Until now, platforms could simply put it on their TandC boards. And get the sink permission to use the data when and how they want. But this approach just doesn't cut it. According to the DPDP Act, you can only use the information for the purpose for which the user has agreed. To get consent, you need to ask your customer: "Hey, I want to use your data, can I? Read this easy-to-use notice, it tells you what data I want to collect and why, i.e the 'purpose' for which I intends to use the data." Consent must now be clear and specific - if you took my data to facilitate a payment transaction, you can justify using it in charge, fraud, refund, and other disputes. All this has to do with one goal. You do not need to obtain separate consent for each such use. But if the target was too broad—like the kitchen sink—that doesn't get in the way. It all depends on whether you can show a clear and specific agreement to achieve a specific goal. But what if you want to use the payment information for a completely different purpose? It’s like selling an insurance policy in a cross-selling fashion.

- If you take a single consent from a customer where the customer says, "You can use my data to provide me this service and show me new products from you or your partners", that combined consent must not violate it. But if the user says, "You can use my information to provide this service" and with another checkbox "You can use my information to send me new offers or new products" - it can work.

- If the new usage is retroactive, i.e. you never mentioned it in your original notification (to the user), then no, you can't use it. Again, you need to ask the customer some variation - "Hey customer, we want to show you new product offers. Can we do that? Our partners sell some of these products. Can our partners get in touch with you? Cross-selling also has two parts: First, showing the customer personalized ads/promotions/offers about the new product. Second, the user journey when the user finds the incentive and interacts with it. In the in the latter case, the user is already engaged with the platform, so you can notify. and gives consent here. But in the former, the user has not yet seen the new product offer - you only want to show a personal incentive - so there is no way to receive consent or notification Then things get complicated.

## Penalties for non-compliance

- When there is a failure to prevent a personal data reach: - Up to INR 250 CRORE.
- Failure to notify the breach to the board and data principle: - Up to 200 crores.
- While processing children’s data the obligations were not fulfilled: - Up to 200 crores.
- Data fiduciary did not fulfil the obligations Up to 150 crores.

The Board, established by the Central Government, will be the statutory body responsible for enforcing the Act. The Board's powers and functions include issuing guidelines and regulations, determining non-compliance, imposing penalties, issuing directions to remedy harm, and investigating violations.[1]

In the Case of Praveen Arimbrathodiyil v.s UOI 2021 [2] The Union Government published a set of regulations in 2021. Using the authority granted to it by Section 87 of the IT Act of 2000, the Information Technology (Intermediaries Guidelines) Rules, 2011, are replaced by these regulations. The government aims to control internet streaming services, social media intermediaries, and digital news outlets through these regulations. According to these regulations, social media intermediaries must adhere to the laid down internal grievance redressal process. In circumstances of significant offences, these intermediaries are also compelled to provide the government with the details of the person who sent the offensive communication. Under the guidelines, intermediaries who violate them forfeit the protection granted to them by Section 79 of the IT Act. As stated in the guidelines, intermediaries who violate them forfeit the protection granted to them by Section 79 of the IT Act. The regulations also mandate that the digital news media establish an internal grievance redressal system and adhere to an ethical code of conduct. In this case, several companies, including WhatsApp, Quint, Live Law, and the Foundation for Independent Journalists, have contested these regulations. The outcomes of the judgement will impact the future direction of Indian law in information technology, for which the petition is currently pending before the Supreme Court for listing.

What effect will the IT Act have?

The Information technology Act of 2000 does not deal with various types of the cyber crimes such as cyber stalking cyber fraud, theft of internet time nor does it have provided any protection as to privacy or the content control which are important concern of the present time. This Act will work co-extensively with that of the IT Act which will together work as strong shield against protection of the data over the internet.

## CONCLUSION

Although the DPDP Law is the culmination of more than five years of debate and reflection, it marks the beginning of the legal regulation of personal data protection. Regulatory developments and institutional arrangements in the coming years will determine how well (or not) personal data privacy is protected. The new law provides the necessary scaffolding, but it is not sufficient for effective data protection. It is debatable whether earlier versions of the draft law would lead to better privacy protection in any substantive way. However, the changes in the content of different versions of the law indicate a changed approach of the government to the protection of privacy. Additionally, the current version of the law imposes much lower costs on Indian companies than before.

The law itself is generally modest and pragmatic. It's welcome. However, in some cases, this is extremely true, which can harm privacy interests. The fact that the central government has significant discretion over substantive matters depends a lot on how well the government commits itself to protecting privacy. Data protection rules are for individuals and privacy protection and ensures that organizations process personal data responsibly. Since my last update in January 2022, several countries and territories have implemented laws such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. Opinions on privacy laws can vary, but they tend to focus on the following key points: Privacy protection: Many people value privacy laws because they improve privacy protection. A person has the right to know how their data is used, and the right affects whether it can be processed or not. Increased responsibility: Data protection legislation imposes obligations on organizations to process personal data responsibly. This includes obtaining clear consent, implementing security measures, and

[1] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-Deloitte-PoV-The-Digital-Personal-Data-Protection-Act-16.08-noexp.pdf

[2] https://blog.ipleaders.in/data-protection-laws-in-india-2/

notifying individuals of any data breaches. Challenges for businesses: Some businesses express concerns about the compliance burden and potential impact on their operations. Compliance with data protection legislation can require significant investments in technology and personnel. Global impact: With the globalization of businesses and digital services, it can be difficult to comply with different data protection rules in different regions. Some argue that more uniform global standards are needed. Empowering individuals: Data protection legislation gives individuals more power over their personal data. This control can help build trust between individuals and the organizations that collect and process their data. Enforcement and Penalties: Opinions vary on the severity of enforcement and the severity of penalties for violations. Some argue that strict enforcement is needed to ensure that organizations take data protection seriously, while others may express concerns about potential overreach. It is important to note that opinions on data protection laws may depend on the context and change over time as these laws are implemented and their impact becomes clearer. Public debate, legal challenges and technological developments also influence the formation of opinions on data protection.