Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Balancing E-Commerce and Data Privacy in India – An Analytical Study

[1]Sowmya Sharma PM, [2]Dr. Chanjana Elsa Philip
[1]Research Scholar CMR University, School of Legal Studies
[2]Associate Professor, CMR University, School of Legal Studies

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

The rapid growth of E-commerce sector in India shows the complex challenge in balancing its immense economic potential with fundamental rights to data privacy. This article details the interplay between the rapid growth of online transactions and evolving data protection landscape in India, particularly in the light of Digital Personal Data Protection Act (DPDPA) 2023. This Article examines the legal framework governing collection, processing and storage of personal data by E-commerce entities. It also explains the status of data privacy laws in India and make suggestions on how there could be a better balance between the rights of use and ownership of data to foster continuing innovation and growth of digital commerce without endangering the consumers. This article calls for the continuing reform and integration process to establish improved framework of eradicating or at least minimize existing inequalities and improving the data protection in India.

Keywords: eradicating, continuing, inequalities, improving

INTRODUCTION

The growing adoption of e-commerce platforms has undoubtedly revolutionalised the face of India's economy and introduced prospects that, on the other hand, cannot pledge the protection of citizens' privacy in the cyberspace. India, the rising global Digital economy, has a high-stakes problem of respecting and safeguarding the fundamental human right to privacy of citizens and consumers. An important concept of data protection regulation has been observed in India between the years of 2017 to 2025 through various crucial judicial judgments and policies.

The two objectives to support the growth of e-commerce and at the same time enhance data protection challenges are associated with many legal, technical, and technical, legal, socio-economic and political factors. Though it has benefited in the areas of Digital Inclusion along with Empowerment of the Indian economy, e-commerce User beware of the potentially damaging risks including data theft, unauthorized use and sale of their data and misuse of their personal information.

This paper seeks to assess the adequacy of the above-stated objectives of India's data protection regime by assessing the extent to which it fosters consumer confidence, promote propriety use of consumer data, and overall promote fair competition among the ecommerce companies. This study aims at evaluating measures that can be taken and or areas to focus in order to strengthen the existing regulations with an overall view of developing a sustainable and secure e-commerce sector.

Ecommerce has assumed a rapid growth in India and has been responsible for growth in several aspects including the increase in choices available to consumers as well as creating the expansion of new markets for business. But, it has also posed several issues to the question of data privacy, rendering it as paramount essentiality to achieve an optimum measure of economic development without compromising the rights of individuals to privacy. This issue requires a legal research analysis of the following reasons.

First, the situation with India E-commerce is that it is highly developed with millions of users performing purchases online daily. This leads to accumulation and consolidation of a vast amount of personal data; thus becoming a concern in terms of data protection. It is therefore important to have legislation to govern all these so as to ensure the

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

consumers are safeguarded from misuse of their data in a way that may lead to acts such as identity theft, unauthorized surveillance, among others.

Secondly, as it has previously been pointed out, India lack information security legislation that can be regarded as unified and up-to-date. While, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 & The Personal Data Protection Bill 2019 are a step in the right direction, this too require enhancement with time which is instantaneous with technological revolution & strictly in accordance with international standards. A legal review can detect the existing legal loopholes and discrepancies in the laws governing the data protection and suggest the sound legal framework that is compatible with the global standards, for instance, the GDPR of the European Union.

Third, one must consider that the pro- and anti- e-commerce legislation is not only the question of laws but it also has economic aspect as well. Such uncertainty is not good for the businesses engaged in the e-commerce industry while regulating consumer rights and protecting consumers. Legal certainty can increase investors' trust and attract Indians and foreign investments into the nation's digital sector. On the other side, good legislation and policies for data protection also increases consumer confidence to carry out their activities through e-commerce market which in return increases the market growth rate.

Therefore, it is critical to discuss legal factors of data privacy in India as well. The problem is that the population of India is highly heterogeneous regarding the level of using digital technologies and knowledge of the rights to data protection. While deciding about the further legal actions, one must involve educational and informative activities that would inform the public out there of its rights and protections.

Finally, the dangers of trading internationally are that the various Indian e-commerce companies must adhere to international data protection practices to transact in international markets. It is thus essential to have a comprehensive legal review of the Indian privacy laws to conform to the international standards for trade and collaboration.

Thus, it is essential to conduct a comprehensive legal investigation into the conflict of e-commerce and data privacy in India based on the necessity to defend buyers, develop the economy, maintain legal harmony, consider social effects, and conform to global trends. Any given analysis on this subject will help the policymakers, businessmen, and stakeholders regarding the arising novel problems in the digital world without compromising individual rights to privacy.

E-COMMERCE INDUSTRY IN INDIA

The use of smartphones and the internet has skyrocketed in India in the past few years. The number of wireless internet subscribers in India increased from 941.5 million in October 2024 to around 944.7 million in November 2024. There has been a meteoric rise in the number of people using smartphones, with an anticipated 1.1 billion units sold by FY25. The digital sector in India has benefited from this, and experts predict that it will reach $1 trillion by 2030. A combination of factors, including increasing disposable incomes and the number of people using smartphones, has contributed to the expansion of India's e-commerce market. The growth of India's e-commerce sector has revolutionised the country's commercial landscape, facilitating interactions between businesses and consumers in a variety of settings, including B2B, D2C, C2C, and C2B. The business-to-consumer and direct-to-business markets have grown at an astounding rate in the last several years. With a predicted CAGR (compound annual growth rate) of 15%, the e-commerce business in India is expected to expand from its FY24 valuation of Rs. 10,82,875 crore (US$ 125 billion) to FY30 valuation of Rs. 29,88,735 crore (US$ 345 billion).

The sector is projected to reach Rs. 47,64,650 crore (US$ 550 billion) by FY35, driven by increased digital use and altering customer behaviour, according to a joint analysis by real estate consulting firm ANAROCK and retail news site ETRetail. Predictions indicate that the beauty and personal care (BPC) industry in India would achieve a gross merchandise value (GMV) of 2,60,610 crore (about $30 billion) by the end of 2027. Just 5% of the world's cosmetics are made up of this. It is the fastest-growing BPC market among major economies, with a growth rate of around 10% each year.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

DATA PRIVACY IN INDIA

Historical Analysis of Data Privacy Act in India

- Early Frameworks and Limited Protections (Before 2000)

Data privacy was not a main issue for the people of India in the pre-internet era since the personal data collection was merely confined to the governmental records. At that time, there were no specific acts pertaining to privacy and data protection where the issue was protected under the Indian constitution and mainly under Article 21 that guarantees both right to life and liberty. It gave a basic, albeit indirect, safeguard to personal information at this point. This IT Act that was passed in 2000 was a first step towards establishment of privacy in India. The first India law that recognised the digital activities was the Information Technology Act, 2000 although it was enacted in 2000. It was added in 2008 whereby Section 43A provided that organization that processed sensitive information was required to employ reasonable security measures. Further Section 72 offended access or divulging of information which was with the government officers or the intermediaries. Nevertheless, it had weaknesses, such as insufficient definitions of "personal data" and "consent", with the goal of protection against cyber threats over the protection of the personal data of individuals.

- Supreme Court Intervention — Right to Privacy Recognized (2017)

The object of present concern has been first legally included into the list of fundamental rights for the citizens of India through the judgement of Supreme Court in the year 2017 in the case of K S Puttaswamy & anr vs Union of India & ors. This particular decision paved way for the need to have a data protection law since it paved the way for the formulation of a comprehensive privacy law in India.

- Draft Personal Data Protection Bill (2018)

To replace the repealed Section 66A of the IT Act, the Justice B.N. Srikrishna Committee was formed to specially draft data protection law. In September, 2018, the committee formulated this draft Bill associated to some provisions like consent for collection of data, localization of data by storing a copy within India. It also provided for the establishment of a Data Protection Authority (DPA). However, the draft has some concerns like, there is new loophole to grant broad exemptions that are based on the dignity of a national security clause and there is also suspicion on the aspect of surveillance.

- Personal Data Protection Bill, 2019

Later on, the government presented a more refined Personal Data Protection (PDP) Bill in the Parliament than the one was introduced in 2018. They included the categorisation of data into special, protected, and essential data; and the subject's rights such as data subjects' right of access, rectification, erasure and portability. Data fiduciaries or data processors were introduced and the latter had new responsibilities. However, the opponents saw it as bill that gave too much power to the government and, as for the DPA, had very limited autonomy. It was forwarded to the Joint Parliamentary Committee for consideration of further action by the parliament.

- Withdrawal of PDP Bill (2022)

In August 2022, there was the removal of the 2019 PDP Bill in line with JPC recommendation which included 81 changes. It pointed out its desire to produce a further 'sophisticated' framework which would cover relatively newer means such as artificial intelligence and block chain.

- Digital Personal Data Protection Act, 2023

In August 2023 the law on Digital Personal Data Protection Act was enacted and some of the measures that were implemented include consent based processing where a particular data subject's consent is required and must be prior, unambiguous, and enlightened. He strengthened the accountability of data fiduciaries dealing with a lot of PII and augmented the rights of individuals such as the right to access, amend, lodge complaints, right to opt-out and others. The Act provided that the Data Protection Board of India would have jurisdiction over disputes and that

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

certain breaches would attract a penalty of up to ₹250 crore. However, despite these reforms, the Act has provided wide powers to the State agencies under certain exceptions.

The following are some of the provisions of the DPDP Act, 2023, as the following are as follows:

1. Data Steward of E-commerce: E-Commerce organizations can be considered as data stewards since they become the legal custodians of individual's information. The Act requires that such companies' approach personal data processing in a transparent manner and only if prior consent has been obtained from the data subject, and for a particular purpose that is both expressly stated and lawful.
2. Consent and Withdrawal: One must not collect, use, or share the personal information of a client involved in e-commerce operations, or related operations, without the latter's prior consent. Subscribers also have the right to revoke their consent which must also be possible for the companies.
3. Data Subject Rights: The Act gives various rights in relation to data, to its subjects or data principals as they are called in the Act these rights include right of access, right of rectification, right to erasure and right to data portability. The implementation of these rights requires strategies that various e-commerce companies should incorporate to enable users to exercise such rights.
4. Data Localization: The Act may contain provisions that would compel various forms of data to be located and processed within the territory of India. This indicates that e-commerce companies may have to establish their local data storage centres or have to conform to such standards.
5. Security and Breach Notification: Electronic commerce enterprises for savings and credit co-operative societies shall put in place adequate measures for securing the data of their clients. There are strict rules that force them to inform individuals whose data has been violated and the regulatory body too within a short span of time.
6. Cooking and Tracking Technologies: The use of cookies and tracking technologies is a matter governed by the Act. Such technologies should be described by e-commerce platforms before using and get the approval from the users.
7. Non-Discrimination: The second principle which relates to discrimination is prohibited based on data-related decisions by data fiduciaries. In implementing this right, the companies using algorithms and processing data must ensure that no discrimination against users is achieved.
8. Children's information: Additional measures are provided for processing of information of and identifiable from children. Some type of data can be processed only with verifiable prior consent of a parent or a legal guardian, which must be provided by e-commerce platforms if the user is under a certain age.
9. Accountability and Compliance: This Act also imposes some accountability measures of the companies which include record keeping of the data processing activities and Data Protection Impact Assessments (DPIA) that is necessary when the processing is likely to be high risk.
10. Supervision: Supervision of the Act is done by a Data Protection Authority (DPA). It indicates that e-commerce companies may require the interaction with the DPA on the issues related to compliance with the legislation and reporting.

Navigating the Digital Landscape: The Impact of Increasing Online Transactions on Data Protection in India under the Digital Personal Data Protection Act (DPDPA) 2023

With its requirements for data minimisation, informed permission, purpose limitation, and stringent security measures to safeguard customer data, the Digital Personal Data Protection Act (DPDP Act) of India has a substantial influence on online commerce. Data should be accurate, kept up-to-date, and deleted when no longer needed; e-commerce companies should only acquire data for certain objectives. Serious consequences, including fines of up to ₹250 crore, may ensue from noncompliance.

The exponential increase in on -line transactions in India has transformed various sectors, facilitating trade, banks and social interactions and conventional paradigms. This digital revolution, characterized by convenience and

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

immediacy, comes with significant challenges, particularly in relation to data protection. Digital Personal Data Protection Law (DPDPA) 2023 represents a fundamental legislative response to growing concerns involving personal data security and privacy in the context of this growing digital scenario.

As online transactions proliferate, the volume of personal data collected, stored and processed by various entities, from e-commerce platforms to digital payment systems, has increased. This vast accumulation of data inevitably increases the risk of data violations and misuse, leading to a pressing need for robust structures to protect users' privacy. DPDPA seeks to address these risks, establishing comprehensive regulations governing personal data processing, requiring user transparency, responsibility and consent.

One of the main impacts of DPDPA is the paradigm shift that promotes in relation to data property and the user agency. Previously, a significant portion of personal data was often collected without explicit consent, leading to a crisis of confidence between consumers and service providers. The DPDPA enshrines the principle of informed consent, requiring entities that collect personal data to obtain a clear and unambiguous permission of data subjects. This requirement not only enables users, but also exhorts organizations to adopt ethical data practices by promoting a safer and more transparent on -line environment.

In addition, the law delineates strict obligations for data fiduciary, responsible for ensuring the security and compliance of personal data processing. By imposing penalties for violations and demanding that organizations name data protection officers, DPDPA enhances responsibility and encourages companies to prioritize data protection. This regulatory structure is essential for the cultivation of a data protection culture among companies involved in on -line transactions, thus mitigating the risks associated with misuse of data.

DPDPA also presents the concept of data location, which requires certain categories of personal data to be stored and processed in India. This provision aims to reinforce national security and ensure that data from Indian citizens are subject to domestic legal protections. Although the location of the data has its merits, particularly in protecting confidential information on foreign jurisdictions, it also raises concerns about compliance costs and operational complexities for companies, especially small and medium -sized companies (SMEs). These often poorly equipped entities to navigate the evolving regulatory landscape can be at a competitive disadvantage, leading to requests for balanced and pragmatic implementation of DPDPA provisions.

In addition, the law encourages the establishment of the Indian data protection board, an independent regulatory body in charge of awarding disputes related to violations and data violations. This institution is ready to play a crucial role in defending the rights of individuals and in the application of responsibility between organizations. The effectiveness of the board will largely depend on its operational capacity, experience and the resources allocated to it, emphasizing the need for a well-supported structure to manage the increase in cases of data protection arising from the increase of online transactions.

As India continues to adopt digitization, the interaction between technological advancement and data protection will remain a focal point of public discourse. DPDPA implications extend beyond mere compliance; they cover broader questions related to trust, innovation and economic growth. By promoting a safe on -line environment through effective data protection mechanisms, DPDPA can increase consumer confidence, encouraging the increase in on -line transactions and, consequently, stimulating economic activity.

In conclusion, increasing on -line transactions in India requires a robust data protection structure, as highlighted by the 2023 Digital Personal Data Protection Act. By promoting user consent, imposing rigorous obligations on data fiduciary and establishing regulatory supervision, DPDPA aims to address the vulnerabilities associated with data collection and processing. However, the success of these provisions depends on collaborative government efforts, companies and consumers to create a safe digital ecosystem that protects privacy and promotes innovation and growth in the growing On -Line market. The continuous evolution of data protection laws in India reflects a critical response to the country's digital transformation, emphasizing the urgent need for a balanced and effective approach to data privacy in the age of digital commerce.

The legal framework governing collection, processing and storage of personal data by E-commerce entities in India

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The wave of e -commerce in India has led to a growing concern regarding the collection, processing and storage of personal data of various entities in this sector. This phenomenon raises significant questions about consumer privacy, data security and legal compliance. The legal structure that governs personal data in India remains in a state of flow, characterized by the evolution of legislative and regulatory measures that deal with the rapid pace of technological advancement and digital commerce.

A crucial component of the legal structure is the 2000 Information Technology Law, which provides the basis for data protection in India. Although initially intended to promote e -commerce and cybercrime legislation, the law also covers provisions on personal data protection. Section 43A of the law requires compensation because it does not implement reasonable security practices, illustrating legal obligations placed in companies that collect personal data. However, the scope of IT law is limited, without comprehensive data protection measures, requiring supplementary regulations.

The Personal Data Protection Bill (PDPB) represents a significant legislative development, with the intention of filling out the gaps in the current structure. Introduced in 2019 and subsequently amended, this bill echoes the principles derived from global standards, particularly the General Data Protection Regulation (GDPR) of the European Union. PDPB outlines data types and establishes critical definitions related to personal data, data controllers and data processors. It requires the explicit consent of individuals for data collection, granting rights to them as access to data, rectification and deletion. Despite its recognition, the project highlights the challenges related to the balance between personal data rights and the operational flexibility of e -commerce entities.

Another vital legal framework is the role of the India Reserve Bank (RBI) in the regulation of payment data. With the increase of various payment platforms, the RBI released guidelines related to data storage and processing, requiring all payment data to be kept in the Indian territory. This regulation, although intended to protect consumer financial information and reinforce national security, presents challenges for companies with global operations that should reconcile these local regulations with international data transfer laws.

E -commerce entities face various challenges of compliance amid this evolving legal scenario. The ambiguity in the definition of personal data and the intricacies of consent requirements complicate operational practices for companies. In addition, small and medium enterprises (SMEs) may have difficulty allocating resources to comply with intricate data protection laws. The lack of a centered regulatory organ specifically for data protection exacerbates the execution challenges, leading to different interpretations of compliance obligations between different jurisdictions

By addressing compliance mechanisms, the PDPB describes the establishment of a data protection authority (DPA), which will supervise the implementation of data protection laws, investigate violations and judge individuals' complaints. However, as this authority has not yet been operationalized, the current regulatory environment remains fragmented. Until DPA is in force, compliance mechanisms depend mainly on self-regulation in the sector, where e-commerce entities are encouraged to adopt best practices for data protection, including the implementation of robust cyber security measures and the development of transparent privacy policies.

Another challenge is the public awareness and understanding of data protection rights. Many consumers are unaware of their rights under existing structures, thus compromising their ability to make informed choices about their personal data. As a result, a double approach to legislation and public education is essential to promote a data protection culture, where individuals are more proactive in affirming their rights.

In conclusion, the legal structure that regulates the collection, processing and storage of personal data by e -commerce entities in India is still emerging. The main laws, such as the Information Technology Law and the Personal Data Protection Law, create a basis for data protection, but significant challenges persist in relation to consumer compliance, application and awareness. As India's e -commerce scenario continues to evolve, it is imperative for legislators, regulators and stakeholders of the sector to contribute to strengthening data protection mechanisms, ensuring that consumer rights are fortified amid the digital trade revolution.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Data privacy challenges faced by E-commerce Industry

Like the e-commerce of other countries, the data privacy in India e-commerce industry has been exerted with some challenges. Such issues are as a result of growing online transactions, vast data about the people collected and changing regulatory environment. Some specific e-commerce data privacy issues witnessed in the Indian context are as follows:

1. Regulatory Compliance:

- Personal Data Protection Bill (PDPB): Continuing with the communication business norms of e-commerce firms, it is necessary to abide with the Personal Data Protection Bill which regulates the data protection and privacy of an individual. The nature of compliance entails the knowledge and adherence to strict data protectiveness rules.
- State Laws: Some states of India might have certain laws related to data privacy and policies which the e-commerce platforms might have to follow or consider the state laws.

2. Data Localization:

- The Indian government has in recent years introduced more rules and regulation as regards localisation of data, that some data should be stored locally in India. This can prove to be cumbersome in terms of practicality and cost especially for online businesses especially the international ones.

3. Third-Party Data Sharing:

- Most of the e-commerce companies employ third-party providers and merchants, delivery firms, advertising agencies and other service providers. It is relatively difficult to guarantee that such partners ensure data privacy compliance and to protect such data during the exchanges.

4. Consumer Awareness and Consent:

- Some customers in India still may not be adequately informed about risks associated with data and data sharing or repercussions of data sharing. Informing people about the purpose and ways data will be used may be difficult due to Issues of collecting informed consent.

5. Data Breaches and Cybersecurity:

- Such threats may have an impact on data and involve possible consequences for both customers and corporations. Internet marketing demands noticeable security mechanisms for the safeguarding of customer information and particularities from hackers and malicious attacks.

6. User Authentication and Fraud Prevention:

- One of the difficult tasks that need to be accomplished is the proper balance between the security level in regard to the authentication processes and the user experience. While applying the strong authentication, which would help to reduce the rates of fraud, can sometimes hinder the user experience due to some extra steps introduced in the process.

7. Handling Sensitive Data:

- A lot of consumers purchase goods and service online using and sharing personal information, credit card details, and other sensitive details through e-commerce platforms. It is, therefore, important to safeguard this data to avoid falling prey to the vice and to enhanced to conform with Payment Card Industry standards.

8. Cross-Border Data Transfers:

- An important reason is that most e-commerce companies function on a global level and therefore transaction of data occurs across borders. Atul Bansal and his team will be able to mindful of these laws and navigate the legal to ensure the protection of data as per Indian and International laws.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

9. Anonymization and Data Minimization:

- For this reason, anonymization and data minimization need to be integrated correctly to safeguard users from exposure. Nevertheless, it is a known fact the accomplishment of all these can be a nightmare especially with regard to service quality and personalisation.

10. Technology and Infrastructure:

- Despite the potential return on investment, implementing, adapting and managing technology and inherent processes for data protection, compliance and efficient data handling require capital and resources.

To overcome these challenges, more effective protections must be put in place by the e-commerce companies in India, it is necessary for the e-commerce companies to know and ensure they meet all the requirements of the existing laws, and companies must ensure they are transparent in their use of the data.

BALANCING E-COMMERCE AND DATA PRIVACY IN INDIA

The passing of DPDP Act in 2023 can be considered as the significant progress made by India in the direction of data protection regulation. It is the first data protection law in the country and has been introduced to seek to counter the emerging trends of data protection especially in e-commerce. The DPDP Act gives a systematic means as to the way personal data is gathered, analyzed and stored so that people's privacy can be honored and safeguarded.

Regarding e-commerce, the role the DPDP Act has is to ensure that consumers have faith in buying products from businesses. When completing purchases or otherwise engaging in shopping activities through the internet, the consumers feel vulnerable and anxious to their information being exploited. Consent is another requirement imposed on businesses by the DPDP Act so that the consumers can comfortably give their consent in way that allows them to control their information. This helps to make the environment more transparent for the companies as well as makes e-commerce organizations more accountable.

Additionally, the DPDP further provides severe consequences for non- compliance and this acts as an advocacy for the protection of data. There is an urge to protect personal data from being breached and accessed by unauthorized individuals in organizations. This is especially so given that the e-commerce sector deals with large quantities of information that is vulnerable to fraud. This is WHERE the measures provided for in the general part of the DPDP Act seek to reduce the likelihood of data breaches that can be detrimental to the consumer and business entities .

People face difficulties in completing an e-commerce affair without compromising on the data subject's rights but the DPDP Act can act as a guideline in dealing with the problem. The legal requirement in e-commerce firms is not only a compliance matter but also a competitive imperative. Consumers are inclined to follow the path of shared motto that can automatically lead them to the desired goal, and by repeating, that businesses can prove that they are dedicated toward protecting their privacy data in the market. The act also promotes data minimization, which means that the firm should collect only the necessary data and must retain it for a legal purpose.

Thus, the DPDP Act is a positive development towards the integration of e-commerce growth with the need for data protection in India. Due to the setting up of such rules and regulations, it seeks to safeguard client information while at the same time promoting the growth of organizations in a world that is increasingly becoming digital. Therefore the DPDP Act will prove to be a significant guiding factor for the formation of a secure e-commerce environment as digital transformation progresses.

Lacunas in the DPDP Act 2023 in relation to e-commerce

The DPDP 2023 of India, is a much-needed bill that seeks to offer protection to Personal data in the current age. Nevertheless, there are several loopholes in the act and unfortunately, concerning e-commerce platforms, the gaps must be discussed and closed for an effective data protection in the country.

The major weakness of the DPDP Act is that it includes no specific provisions to regulate the gathering and utilisation of data by e retail outlets. The act though covers the processing of personal data does not offer specific directions to e-commerce businesses on how to properly manage the vitals that belong to the consumers such as financial

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

information, data on their location, or data on the sites they frequent. Lack of specificity may cause different meanings for the same term and consequences in the forms of inconsistent application of rules across various or most e-commerce platforms which put the consumer data at risks.

There is no clear provision as to where the data is to be captured and stored and this is what we will call the data localization and storage provision. The DPDP Act does not plainly specify where personal data collected within e-commerce was prescribed to be processed and stored. Since the data is transmitted over the internet to different parts of the world when it is on cloud, issues of jurisdiction and control over data come into play. If there were no strict data localization regulation in the region, the data could be shifted to other countries that do not have strict data protection laws thus posing danger to the users" private information.

It also lacks correct means of seeking user consent and giving account of the e-commerce transactions. Although it entails the consent of the data subjects, it does not explain how the e-commerce platforms should let the users know about collection of their personal information or how they can get the imperatives consent; especially when the consent is surreptitiously obtained through cookies and other tracking technologies. This can lead to such situations where consumers are enclosed from the extent of data collecting hence they will be unable to make rational decisions.

In addition, there had been no clear provisions made in the DPDP Act in regard to conditions of sharing of data and access to it by other third parties. Traders from the e-commerce market often disclose their consumers' information to third parties to perform different operations, for example, taking payment, promoting products, or shipping merchandise. As for the data sharing, unfortunately, the act does not contain a detailed explanation of how that should be done and what responsibilities should be put on the third party that processes data for e-commerce businesses. This generates a chance for companies to abuse or misuse the collected consumer data with little legal consequences.

Finally, the act lacks adequate provisions to do with breach notification and response. More so, it is equally ambiguous on the time, and procedures to use when informing the users or the authorities of the loss of such data. Such provisions are important in containing impacts of data breaches, of which have became a norm in the digital world, and to quickly contain them. There should be some guidelines concerning how these MEPs should deal with the breaches to foster consumer confidence and give them a legal way to regulate themselves.The DPDP Act of 2023 as proposed can be considered as a positive step towards data protection; however, it needs further improvements in order to adequately address the concerns arising from e-commerce activities. In filling these gaps it will assist in enhancing the act to support the privacy and security of the consumers' data which is a crucial factor due to the advancement in e-commerce.

DISCUSSION

The research acknowledges the current and prospective dynamics of the Indian e-commerce industry regarding data privacy regulation and reveals strengths and weaknesses that, in the Stephanie Authiray's opinion, require further attention. There is one more focus area, namely regulated non-clarity, especially in the sphere of the Personal Data Protection (PDP) Bill. For instance, while the GDPR provides great detailed guidance concerning any possible implementation, the PDP Bill provides minimal general guidelines, hence resulting in different interpretations among the organizations. This is because regulatory policies are often ambiguous, and this requires the Indian authorities to provide clear and precise directions to reduce the formation of numerous interpretations and improve the standard of the guidelines.

This has led to a differential between the large multinational organisations particularly in the world of e-commerce and SMEs in the implementation of data protection. However, due to their dominance of human and material resources, multinational firms can obey the act decently while SMEs have it tactically hard, this also affects the consumers' rights and the competition fairness. It is believed that adopting appropriate practices of data protection needs sufficient support in the form of technical support and funding and the SMEs should be trained adequately on how to implement proper data protection mechanisms.

While these policies are usually aimed at protecting the nations' sovereignty, interests and/or revenue, they disrupt the global digital business by limiting the cross-border data flow and raising the price of operations. A middle

approach, for example through non-disclosure agreements on exchange of data with sound protection measures, is more possible of realizing both national security interests as trade internationally. In the same way, change of the regulatory approach from a reactive one, focused on the identification of potential risks and resolving them as soon as possible is needed. The systems of monitoring continuous can be used along with investing in cybersecurity to prevent data breaches and restore consumer trust.

The study also highlights the weakness of cross-jurisdictional alignment because the current legal framework governing data privacy in India remains aligned with the international standards such incongruity makes the compliance of data privacy regulation difficult besides hindering the protection of consumers rights. A specific policy compliance with global regulatory norms of data protection would help improve international business between India and other countries and make the laws much easier to forecast. In addition, due to tremendous innovations in the technology industry, there is unfixed rate of change. Discussing AI-based risks is incomplete without mentioning its benefits as well as risks for data privacy and protection. Implementation of an innovative regulatory sandbox concept for policy testing and development with the stakeholders of the industry could be considered as the best approach which would call for proactive rather than reactive regulation.

CONCLUSION

The e-commerce industry in India has grown rapidly in the last decade in that it has set up India as a prominent player in the worldwide e-commerce industry. This surge, however, has raised data privacy as a significant factor that needs to be addressed and put into consideration. While e-commerce platforms gather a massive amount of individuals' data, they face multiple issues concerning data protection, such as the proper protection of the information, consent acquisition processes, and legislation differences. This is due to the massive growth in the growth and technological advancement in this sector, which makes it easier for hackers to breach into organizations' data, unauthorized access and misuse of data. In addition, there are difficulties linked to the expansion of business and the high requirements that govern the use of personal data. Accuracy of data protection is a critical factor to ensure that the consumers input their information in the e-commerce entities they intend to use since consumers are now more concerned with their data rights with the rightful enactment of rules and regulations such as Digital Personal Data Protection Act (DPDP) 2023.

Despite the fact that the DPDP Act 2023 is expected to deepen data privacy in India, it should be noted that it has some gaps, especially with respect to the e-commerce sector. These gaps are the ones that include the issues to do with the definition of consent and the nay large data localization and absence of rules concerning the transfer of data across borders. However, some of the measures of enforcement in the act and the penalties that are associated with it may be inadequate to ensure compliance among the large e-commerce conglomerates. It is therefore important to fill the following gaps for the Act to adequately protect consumers' data and promote a secure online space. Both e-commerce firms and other relevant stakeholders should strive to further clarity, enforcement, and culture when it comes to data principles of privacy. But only when the free market is not just restrained and yet balanced enough to protect the consumer privacy it will only help the e-commerce business in India to grow steady in its way.

REFERENCES

[1] https://corridalegal.com/e-commerce-and-data-privacy/
[2] https://www.ibef.org/industry/ecommerce#:~:text=India's%20e%2Dcommerce%20industry%2C%20valued,(CAGR)%20of%2015%25.
[3] https://www.linkedin.com/pulse/impact-dpdp-act-2023-e-commerce-businesses-dpdpconsultants-y3wsf
[4] K., Kanagayazhini. (2022). Critical Analysis of Data Protection and Privacy in E-commerce. *Issue 6 Indian JL & Legal Rsch.*, *4*, 1.
[5] P., Shwetha. (2021). Comparative Analysis of Privacy and Data Protection Laws in E-Commerce. *Indian JL & Legal Rsch.*, *3*, 1.
[6] Patil, A. (2024). Navigating the Digital Landscape: India's Evolving Legal Framework for E-commerce, Data Protection, and Cyber security. *Data Protection, and Cyber security (May 29, 2024)*.
[7] Chimmili, P. K. (2023). Impact of Digital Personal Data Protection Act, 2023 on Indian E-Commerce. *Legal Lock J.*, *3*, 92.

Research Article

[8] Kashyap, A. K., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. *Law & Safety*, 207.
[9] Sumanjeet. (2010). The state of e-commerce laws in India: a review of Information Technology Act. *International Journal of Law and Management*, *52*(4), 265-282.
[10] European Commission. (2018). General Data Protection Regulation (GDPR). Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en
[11] Jain, R., & Sharma, P. (2020). Data Protection Challenges in Indian Digital Markets. *Journal of Information Policy*, 10(2), 135–158.
[12] Kumar, S. (2020). The evolution of data privacy in India: Policy challenges and regulatory reforms. *International Journal of Cyber Policy*, 5(3), 211–230.
[13] Reddy, V., & Singh, A. (2019). Data Localization in India: Implications for E-commerce and Cross-Border Trade. *Journal of Global Information Management*, 27(4), 45–64.
[14] Verma, H., & Gupta, M. (2021). Bridging the gap: An analysis of the Indian Personal Data Protection framework and its global implications. *Indian Journal of Law and Technology*, 17(1), 88–107.
[15] World Bank. (2022). Digital India: Opportunities and challenges in the e-commerce sector. Washington, DC: World Bank Publications.
[16] Additional data and regulatory reports were sourced from the Ministry of Electronics and Information Technology (MeitY), Government of India, and the Reserve Bank of India (RBI) archives (2018-2023).