PERSONAL DATA PROTECTION AND E-COMMERCE

Keerthana PD, CSI Law College, MG University, Kottayam

Introduction

The e-commerce sector in India has experienced remarkable expansion in recent years. Recognizing India's significant e-retail potential across various segments, investors have actively poured capital into the e-commerce industry. It has successfully connected nations and enterprises, emerging as a vital channel for communication as well as for goods and services in online marketplaces. As a platform, the internet enables and provides an incredibly diverse range of e-commerce business opportunities.

In India, the e-commerce sector has been experiencing significant growth and is projected to overtake the U.S. to become the world's second-largest e-commerce market by 2034. The value of the e-commerce industry in India was around US$ 50 billion in 2018 and is anticipated to rise to US$ 200 billion by 2027[1]. The significant expansion of e-commerce in India over the past twenty years can be attributed to the increased access to the internet and mobile phones among the populace, fostering the rise of online shopping in India.

The personal data plays a crucial role in the functioning of e-commerce by enabling personalized and efficient customer experiences. E-commerce platforms collect data such as browsing history, purchase behavior, location, and preferences to tailor product recommendations, targeted advertisements, and promotional offers, and the customers in the mad driven era of e-commerce are compromising their personal data and privacy for the convenience of digital shopping resulting to the major cyber threats like data breaches, leading to identity theft, scams or phishing attacks ending up in privacy right violations and financial loss[2].

This article upon the light of these recent trend of E-Commerce platforms explores on the existing legal frameworks on the personal data protection in these online platforms, assessing

[1] Channel Engine, https://www.channelengine.com (last visited April, 28, 2025)
[2] Norijhan Abdul Ghani, personal information privacy protection in E-Commerce, Issue 3 volume 6, 407-414 (2009)

their legal lacunas with potential suggestions to address those fallibilities.

E-commerce and personal data

E-commerce has dramatically changed contemporary society by altering the way people shop, engage with businesses, and obtain goods and services. Central to this change is the strategic utilization of personal data, which drives targeted advertising, tailored recommendations, flexible pricing, and improved user experiences. Businesses gather and examine consumer data including browsing history, purchasing patterns, and demographic details to gain insights into individual preferences and enhance their offerings. Although this data-centric approach provides greater convenience and efficiency for consumers, it also prompts concerns about privacy, data protection, and the ethical handling of information, positioning personal data as both a powerful resource and a significant topic of discussion in the digital marketplace[3].

The swift expansion of e-commerce in India during the past twenty years can be attributed to the increasing accessibility of the internet and mobile phones among the populace. The shift towards the digitalization of the Indian economy, along with favorable market conditions, has contributed to the surge in online shopping within the country. Other factors propelling the growth of e-commerce, particularly online shopping, include the availability of internet content in regional languages, advancements in logistics and communication infrastructure, the transition toward cashless transactions, and a positive consumer attitude towards online purchases. Consequently, the number of online shoppers has seen a remarkable rise in a brief period. Between 2014 and 2020, there was a sixfold increase, and India achieved the highest Compound Annual Growth Rate (CAGR) of 70% in online retail sales from 2012 to 2017 among major economies. Nonetheless, by the years 2016-2017, online retail accounted for only 1.5% of the total retail market in India, and this figure rose to 1.6% in 2019, with projections estimating it will reach 8% by 2025[4].

Personal information is vital for the operation of e-commerce platforms, influencing almost every element of how these businesses function and interact with customers. From product suggestions to targeted promotions, logistics to customer support, e-commerce sites depend

[3] Rahmi Ayunda, Personal Data protection to E-Commerce, what are the legal challenges and certainties? 18(2), 144-163 (2022)
[4] Mordor Intelligence, https://mordorintelligence.com (last visited Nov. 8, 2024)

significantly on gathering, analyzing, and using users' personal data. This information encompasses both explicit details like name, email, phone number, and payment information and implicit behavioral insights such as browsing patterns, click behaviors, time spent on pages, and past purchases. Collectively, this data allows platforms to offer a customized shopping experience, enhance customer satisfaction, and boost sales. A prominent application of personal data is personalized product recommendations. E-commerce platforms employ algorithms that analyze users' historical behaviors, preferences, and demographic information to propose items they are likely to find appealing[5]. For instance, Amazon's recommendation system is driven by sophisticated machine learning algorithms trained on extensive datasets of user interactions. These systems not only raise the likelihood of a purchase but also improve user engagement by making the shopping experience more relevant and user-friendly.

Another important application of personal data is in targeted advertising. E-commerce platforms, often collaborating with third-party advertisers, utilize data to segment customers according to their interests, location, age, and purchasing intent. This enables businesses to display customized advertisements across websites, applications, and social media channels, frequently using cookies and tracking pixels. By focusing on a specific audience, these ads become more impactful, improving the return on investment for advertisers while also supporting the monetization strategies of the platforms. Furthermore, personal data is essential for processing orders and managing logistics. Accurate shipping requires users' addresses, contact details, and sometimes real-time location data. E-commerce platforms use this information to optimize supply chain operations, predict delivery times, and create a smooth purchasing experience. For example, data analysis assists in identifying which products should be stocked in which warehouses to reduce both delivery times and costs. Additionally, customer service and support systems significantly benefit from access to personal data. When a user contacts support, their previous interactions, purchase history, and preferences allow service agents or AI-powered chatbots to resolve issues more quickly and efficiently. This not only boosts customer satisfaction but also reduces operational expenses for the platform. Thus, personal data forms the backbone of modern e-commerce. It enables platforms to function effectively, address user needs, and maintain a competitive advantage. However, the heavy dependence on this data demands strong data protection measures to guard against misuse and uphold consumer trust. The rapid growth of e-commerce platforms utilizing consumers'

[5] Forbes, https://www.forbes.com, (last visited. April 29, 2025)

personal data has raised significant concerns about the protection of personal information, as these platforms continuously collect vast amounts of sensitive data, including names, addresses, payment information, and browsing habits. While this data is vital for providing customized services and enhancing user experiences, it also makes e-commerce platforms attractive targets for cybercriminals. Recently, several major data breaches, such as those affecting eBay, Alibaba, and Amazon sellers, have compromised the personal data of millions of users, leading to financial fraud, identity theft, and a dip in consumer confidence. These incidents highlight the urgent need for robust data protection strategies and regulatory measures to ensure users' privacy within the online marketplace.

India's Personal Data Protection

Particular data protection involves safeguarding sensitive information belonging to individuals. In the contemporary digital landscape, where data is frequently gathered, reused, and shared, the protection of personal information has become a critical concern. The importance of personal data arises from individuals' fundamental right to manage their information and their essential right to be protected against various data breaches that could lead to identity theft, financial harm, and damage to their reputation. This principle was upheld in the landmark case of K.S. Puttaswamy V. UOI, which recognized the right to privacy under Article 21 of the Indian Constitution. This decision established a foundation for data protection laws in India, emphasizing the necessity for adequate measures to prevent data breaches. To protect their citizens from such violations, many countries have instituted their own legal frameworks and regulations, such as the DPDP Act 2023 and the CCPA Act 2019, or have joined various international agreements like the GDPR and the Council of Europe Convention 108.

In terms of the legal safeguards for personal data protection, India did not have specific legislation in place for the e-commerce sector until 2022, aside from certain sections of the Information Technology Act, 2000. Particularly, Section 43A requires businesses to adopt reasonable security measures when managing sensitive personal data, while Section 72A imposes penalties for the unauthorized disclosure of personal information. Furthermore, the Consumer Protection Act, 2019, protects consumers against unlawful trade practices, including the improper use of personal data in non-transparent manners. The introduction of the Digital Personal Data Protection (DPDP) Act in 2023 was a response to the urgent need for a comprehensive legal framework to regulate the collection, processing, storage, and

safeguarding of personal data within India's increasingly digital landscape. As internet usage, digital transactions, and online shopping platforms have grown, concerns regarding data breaches, unauthorized data sharing, and the misuse of personal information have escalated. Previous legal frameworks, such as the Information Technology (IT) Act, 2000, and the Consumer Protection Act, 2019, were deemed inadequate in addressing these issues, as they lacked extensive provisions regarding user consent, data minimization, purpose limitation, cross-border data transfers, and individual rights over personal data. Moreover, although the Consumer Protection Act is applicable to e-commerce and illegal trade practices, it did not comprehensively tackle the entire process of personal data handling or establish accountability for those managing the data. The increasing worries about data breaches within and outside the country prompted the government to implement a dedicated privacy law. These legal and societal shortcomings highlighted the necessity for the development of the DPDP Act, 2023, which lays out a rights-based framework for individuals and delineates clear responsibilities for data fiduciaries, thereby promoting higher accountability, transparency, and data sovereignty in the digital era. The Act stipulates that personal data can only be processed after obtaining the individual's consent or for legitimate purposes. Moreover, consent must be obtained solely for lawful reasons. In conjunction with consent, both the personal data in question and the purposes for which consent is granted must be articulated and must be voluntary, informed, specific, and unconditional. The rights of the Data Principal and the duties of the data fiduciary do not apply when data processing is conducted for the enforcement of any legal rights or claims by a court or tribunal, or any other authority in India assigned with judicial, quasi-judicial, or supervisory roles, for the prevention, investigation, detection, or prosecution of any offenses outside India, which is necessary for a scheme involving compromise, arrangement, merger, or amalgamation of multiple companies or entities, or to assess the financial status and assets and liabilities of individuals who have defaulted on payments to financial institutions. Additionally, exemptions include personal data processing in the interests of India's sovereignty and integrity, maintaining friendly relations with foreign countries, state security, public order, and for research, archiving, or statistical purposes. The Act provides specific rights to the Data Principal, including the right to access information regarding personal data, to correct and delete personal data, to pursue grievance resolution, and to appoint another individual to exercise rights in case the Data Principal passes away or becomes incapacitated. A significant feature of the DPDP Act is its penalty provisions. Various fines are imposed on data fiduciaries who fail to comply with the Act's stipulations, with

penalties reaching up to INR250 crore. These penalties include breaches of duty to the Data Principal up to INR 10,000, failures to notify the Data Protection Board and affected Data Principals in the event of a personal data breach, which can reach up to INR200 crore, and violations of additional obligations concerning children up to INR200 crore.

The Data Protection Authority (DPA) will be responsible for enforcing the DPDP Act. The Act's establishment and operation will be crucial for its effective implementation, but challenges remain, as businesses in India continue to adjust to the DPDP Act's stipulations. Many organizations may need to invest in technology and processes to become compliant with the regulations. The DPDP Act contains provisions regarding cross-border data transfers, which will necessitate careful consideration and alignment with international data protection standards. Additionally, the Act imposes various penalties for non-compliance, including fines and imprisonment. The effectiveness of enforcement will depend on the proactive nature of the Act; it presents a complex legal structure that may require significant effort from both businesses and individuals. Aligning India's data protection laws with international standards is vital for facilitating cross-border data transfers. Nonetheless, the DPDP Act represents a notable progress in the protection of personal data in India. While challenges still exist, the successful implementation of the DPDP Act will hinge on several factors, including effective regulation, cooperation from the industry, and technological advancements.

The Digital Personal Data Protection (DPDP) Act, 2023 signifies a key advancement in safeguarding digital privacy in India, yet it has several legal and enforcement deficiencies, particularly in the context of the global e-commerce landscape. One major shortcoming lies in the enforcement framework; the Act grants extensive authority to the Data Protection Board of India, but its independence, operational transparency, and resource capabilities remain ambiguous. Unlike international frameworks such as the EU's General Data Protection Regulation (GDPR), which offers robust regulatory oversight and defined penalties, the DPDP Act lacks comprehensive procedural safeguards and timelines for complaint resolution, which could potentially undermine user rights in practice.

Moreover, the significant exemptions allowed for the State, including provisions that permit data processing without consent under vaguely defined justifications such as public interest or national security, raise concerns about possible government surveillance and erode public trust in data protection efforts. Furthermore, the legislation adopts a narrow focus by prioritizing

digital personal data and overlooking non-digital data and sensitive anonymized datasets that could still be reverse-engineered, which may be exploited by data-driven e-commerce companies.

Given the limitless nature of e-commerce, the Act's regulations on cross-border data transfers are inadequate. It authorizes transfers to specific countries designated by the government but does not establish clear criteria or ensure mutual safeguards, unlike the adequacy framework established by the GDPR. This introduces potential risks when data from Indian users is handled by multinational companies operating in jurisdictions with weaker privacy regulations. Additionally, the absence of precise definitions for key terms such as “harm,” “profiling,” or “algorithmic decision-making” limits the legislation's effectiveness in addressing the emerging challenges posed by AI and data analytics in the global e-commerce landscape.

In conclusion, the DPDP Act, 2023 lays an essential legal foundation for data protection in India; however, it does not sufficiently address the intricate and evolving challenges presented by transnational e-commerce platforms. Addressing these gaps will necessitate the development of robust institutional mechanisms, clearer regulatory parameters, and alignment with international standards to ensure that Indian consumers receive meaningful privacy protections within an increasingly global digital marketplace.

The legal disparities in the personal data protection in and around the globe

In a world where commerce is increasingly digital and transcends borders, safeguarding personal data has become a paramount issue. E-commerce platforms inherently depend on gathering and processing user data to offer personalized experiences, facilitate marketing, manage logistics, and process payments. Nevertheless, differing national legislations and the absence of a cohesive global strategy have led to legal ambiguities and challenges in compliance. To address this, various international legal frameworks and guidelines have been introduced to ensure the secure management of personal data across different countries. These frameworks aim to establish shared principles like consent, transparency, accountability, and security that e-commerce platforms must follow when functioning in various jurisdictions.

One of the pioneering and most impactful instruments in global data protection is the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, first adopted in 1980 and revised in 2013. Although these guidelines are not legally enforceable, they act as

core principles for numerous national data protection regulations. They outline essential privacy principles, including limits on data collection, clear purpose definition, restrictions on data usage, and security measures. For e-commerce platforms, the OECD framework promotes responsible data management practices and fosters the unrestricted flow of data between both member and non-member nations, as long as privacy is sufficiently safeguarded[6].

The General Data Protection Regulation (GDPR), established in 2018 by the European Union, represents the most thorough and enforceable data protection legislation to date. Although it is a regional law, its effects are felt worldwide since it applies beyond borders to any company including online retail platforms that gathers or processes the personal information of EU residents, no matter where the company is based. GDPR sets forth stringent regulations regarding user consent, data minimization, profiling, rights of data subjects, and the transfer of data across borders. Failure to comply can result in significant penalties, prompting global e-commerce businesses to adjust their data management practices to meet GDPR requirements[7].

In the Asia-Pacific region, the APEC Privacy Framework along with its Cross-Border Privacy Rules (CBPR) system offers a collaborative approach to data protection that encourages business innovation. Although it is voluntary, the framework advocates for accountability-driven privacy protection and eases data transfers between participating economies. It provides e-commerce platforms a means to showcase compliance through certification processes, thus enhancing consumer trust and lowering trade obstacles. Despite India's non-membership in APEC, the framework plays a role in shaping broader regional discussions regarding cross-border data governance[8].

The United Nations Guidelines for Consumer Protection (UNGCP), updated in 2015, highlight the necessity of safeguarding consumer privacy in online commerce. They urge businesses and governments to create efficient systems to protect consumer information, encourage informed consent, and stop unauthorized sharing of data. Although these guidelines are not legally enforceable, they serve as a foundational framework for national laws and are particularly

[6] Organisation for Economic Co-operation and Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (2013),
[7] ibid 12
[8] Asia-Pacific Economic Cooperation (APEC), *APEC Privacy Framework*, APEC (Nov. 2005)

significant for developing nations as they formulate their e-commerce regulations[9].

Even with various international regulations in place, there is still no universally binding and harmonized legal measure that specifically addresses personal data protection in e-commerce. The variety of methods spanning from the strict enforcement of GDPR to the optional guidelines of APEC leads to regulatory fragmentation. This situation not only imposes conflicting compliance demands on global e-commerce companies but also weakens uniform protection for consumers. There is an increasing demand for a cohesive global framework or treaty that can balance national sovereignty with international standards, ensuring that digital commerce is built on trust, transparency, and privacy.

The need for International Data Privacy Standards

In a time when e-commerce platforms function across borders with unmatched speed and scale, the urgency for international privacy norms regarding personal data protection has risen significantly. These platforms frequently gather, handle, and transfer extensive amounts of personal data including names, contact details, financial information, and behavioral profiles often navigating through numerous regions with vastly different data protection regulations. This legal disarray creates considerable obstacles for both consumers and businesses. Consumers encounter varying privacy protections based on their location or the sites they shop from, while companies find it challenging to adhere to a fragmented assortment of national laws, which elevates operational costs and legal liabilities. Additionally, the lack of a cohesive global framework erodes consumer confidence, particularly in cross-border digital dealings where transparency and accountability are crucial. Implementing consistent international privacy protocols would guarantee a minimum level of protection for all users, enhance regulatory clarity for companies, and encourage equitable, secure, and inclusive growth within the global digital marketplace. As data becomes the essential component of e-commerce, having harmonized regulations is not merely a preference, it is vital for the long-term health of digital trade.

The primary concern arises from the term consumer, as its precise definition can differ based on the legal jurisdiction and applicable regulations. It's important to refer to the relevant laws

[9] United Nations Conference on Trade and Development (UNCTAD), United Nations Guidelines for Consumer Protection (as expanded in 1999)

and legal resources for a clear understanding in a specific context. In the absence of a universal regulation, various industries or regions may adopt distinct definitions of consumer regarding data protection, resulting in ambiguity and uncertainty for both businesses and consumers. This issue of varying definitions arises from the differing scopes of definitions; for instance, when it comes to personal data, various laws may interpret it differently, creating confusion about which information is actually safeguarded, since some regulations might exclude certain types of data, such as publicly accessible information, while others might include them[10].

Another significant problem that consumers encounter due to the lack of uniformity in personal data protection laws is the Discrepant Data Protection Standards, as various sectors or regions implement their own personal data regulations and frameworks that may offer different levels of protection, resulting in confusion and potential vulnerabilities[11]. This inconsistency in data protection arises from the varying degrees of safeguards, such as sector-specific differences, where industries like healthcare, finance, and telecommunications may enforce different levels of data protection, resulting in a fragmented regulatory landscape. Some industries may impose more rigorous data security standards, while others might have fewer comprehensive protections. Additionally, there are geographical discrepancies, as different regions within a nation may adopt different data protection regulations, causing confusion and uncertainty for businesses that operate across borders. Furthermore, the existing laws may not be aligned, leading to inconsistencies and overlaps that can present compliance difficulties and legal ambiguities.

One significant issue that can be noted is the challenge in enforcing consumer rights, as the lack of a comprehensive law makes it more difficult for individuals to uphold their data privacy rights. Customers may encounter barriers in determining which regulations are applicable, where to lodge complaints, and how to pursue remedies[12]. The lack of a cohesive personal data protection legislation within a nation greatly impairs the successful enforcement of consumer rights. In the absence of a singular law, or due to the presence of various regulatory agencies, different sectors or geographical areas may be governed by different authorities. This results in a disjointed enforcement environment, complicating the coordination of investigations and the assurance of uniform enforcement.

[10] Suzanne C Bernstein, Consumer data protection and privacy, Vol.82, 23-26, 2022.
[11] Ibid 17
[12] Springer, https://www.springer.com, (Last visited. Dec 31, 2024)

The lack of a cohesive personal data protection law in a nation leads to considerable challenges concerning accountability. Without a comprehensive framework, it becomes challenging to identify who is at fault for data breaches or misuse, obstructing investigations and making it difficult for consumers to pursue compensation[13]. The complications arising from unclear accountability stem from the difficulties in assigning responsibility, as various entities, including data controllers, processors, and third-party vendors, may be involved in the intricate data processing ecosystems. In the absence of a definitive framework, pinpointing which entity is liable for data breaches or other infractions can be problematic.

A mix of regulations can lead to discrepancies in data security practices. This situation may heighten the risk of data breaches and jeopardize customer information. Different sectors or regions might impose varying levels of data security obligations, resulting in loopholes and weaknesses within the overall data protection framework[14]. For example, some sectors may enforce more stringent standards for data encryption and access controls, whereas others could have less robust safeguards. Additionally, existing laws may not be coordinated, leading to inconsistencies and redundancies that can create gaps in data security measures.

In today's world of shopping at our fingertips, consumers frequently rely on E-Commerce platforms offering a variety of products both locally and internationally since cross-border e-commerce allows consumers to access a broader selection of items and services globally, often at attractive prices. Online shopping provides convenience and flexibility, enabling consumers to make purchases from anywhere and at any time, which draws them to the idea of cross-border E-Commerce[15]. However, along with these enhanced advantages, there are several challenges and gaps that raise issues regarding security, privacy, and legal protections. Various countries possess different data protection regulations, with varying degrees of strictness and coverage. This results in a complicated legal framework for both consumers and businesses. Shoppers may not understand which laws govern their data when dealing with international companies. Additionally, enforcing data protection regulations across different countries poses difficulties. Consumers might encounter challenges when trying to obtain compensation for data breaches or other infractions if the company is based abroad. Some nations implement data localization laws, requiring specific types of data to be kept within their borders. These

[13] Ibid 17
[14] [14] Deloitte, https://www.deloitte.com, (Last visited. Dec 31, 2024)
[15] Liu Zhuang, The development and challenges of data protection law, Vol.13, 40-43, 2024.

laws can impede cross-border data transfers and restrict consumer access to products and services from overseas businesses.

Hence these lack of clarity can result in loopholes that companies might take advantage of, which could lead to the improper handling of customer information and heightened privacy risks. Discrepancies in the level of protection among various industries or locations create openings that malicious actors can utilize; for instance, if one industry has less stringent data security regulations, it becomes an attractive target for attacks, potentially putting sensitive information at risk across the entire network. Additionally, flaws and inconsistencies in current legislation can establish weaknesses that cybercriminals can exploit to unlawfully access personal information.

Conclusions and Suggestions

Despite the existence of various regional regulations, such as the GDPR in the EU, sectoral laws in the United States, and India's Digital Personal Data Protection Act of 2023, which have made significant advancements in safeguarding personal data, they often operate within distinct legal frameworks. This fragmentation in global privacy laws poses substantial challenges for e-commerce platforms that function across different jurisdictions, complicating their efforts to achieve consistent compliance while providing varying degrees of consumer protection based on location. As digital commerce increasingly transcends traditional boundaries, the risks associated with data misuse, cross-border infringements, and disputes related to jurisdiction are intensifying. Therefore, the creation of a comprehensive international privacy standard is not only relevant but also urgently needed. Such a framework would serve as a cohesive guide, defining universal principles and foundational safeguards while allowing for regional variations. It would facilitate smoother international data transactions, enhance user trust in digital spaces, reduce compliance hurdles for businesses, and uphold the fundamental right to privacy on a global scale. Ultimately, a coordinated approach is vital to address the shared vulnerabilities of the digital age and to ensure that the growth of e-commerce does not come at the expense of individual privacy rights.

Thus, several recommendations and suggestions can be proposed while developing an international standard for privacy in the e-commerce sector. These include establishing a universally acknowledged set of core principles such as legality, fairness, and transparency, as well as enforcing data minimization and purpose limitation, ensuring that only the data

essential for specific objectives is collected and processed. The personal data acquired by e-commerce platforms from users should be handled in a way that guarantees proper security measures, protecting against unauthorized or unlawful use and accidental loss, destruction, or damage. Individuals ought to have the right to access their personal data and to be informed about its processing, in addition to having the ability to correct any inaccurate or incomplete data. They should also have the right to receive their personal data in a structured, widely-used, and machine-readable format, allowing them to transmit it to another controller, and have the option to object to the processing of their data, including for purposes of direct marketing. Advocating for multilateral agreements that establish common standards would facilitate cross-border data flows while ensuring adequate protection for individuals. Encouraging collaboration and coordination among data protection authorities to guarantee consistent interpretation and enforcement of the law, as well as developing an efficient system for settling cross-border disputes related to data protection, can address key issues associated with cross-border transactions. Additionally, creating a regular review mechanism and updates to the uniform law to meet emerging technologies and challenges, alongside offering technical support to developing nations to help them enhance their capacity to implement and enforce data protection laws, will ensure robust enforcement mechanisms that deter non-compliance and enable customers to effectively assert their rights.