Page 825 - 835 **DOI:** *https://doij.org/10.10000/IJLMH.115476*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 4

2023

Personal Data and Consumer Protection in E-Commerce: Examining Laws and Issues

MOHD ABDUL SABUR KHAN[1]

ABSTRACT

E-commerce or electronic commerce refers to the use of Internet services for commercial purposes. The landscape of buying and selling goods and services has changed due to the massive growth of e-commerce and digital penetration, as it has mammoth potential to grow but it also presents a slew of legal challenges to be addressed in order to ensure its fairness and security. The study begins with an introduction to e-commerce and its importance in the era of digitization of business practices. The growth of e-commerce in the last century has made it necessary to have an effective legal system to deal with issues and new challenges. With e-commerce comes the issue of personal data protection of individuals from misusing by the e-commerce web giants, this study aims to address the laws and challenges on personal data protection. Another essential growing concern is consumer protection in the realm of digital businesses, this study intends to discourse the related laws and regulations to protect the interests of consumers in online commercial transactions.

This research study aims to provide a thorough understanding of the current laws and issues in e-commerce by examining privacy and consumer protection, this study aims to contribute to the establishment of an effective legal framework that promotes trust and confidence in e-commerce within the digital realm.

Keywords: *GDPR, DPDP Bill 2022, IT Act, 2000, E-Commerce Rules 2022, UNGCP.*

I. INTRODUCTION

Electronic commerce or in-short e-commerce are Transactions that often entail the transfer of any kind of value recognized by the sovereign and not prohibited by law, through online platforms like websites and mobile applications in exchange for goods and services. "E-commerce has risen rapidly from 15% of global retail sales in 2019 to 21% in 2021 and 22% in 2022. Over the long term, e-commerce can increase to 5.4 trillion by 2026"[2]. With the rising internet penetration and use of electronic devices, consumers now have incomparable access to goods, services, and information. The Internet and the web have played a crucial role in reaching a worldwide audience around the clock and have prompted unparalleled e-commerce with the

[1] Author is a student from ICFAI LAW School, Hyderabad, India.

[2] Morgan Stanley, Here's why e-commerce growth can stay stronger for longer, MORGAN STANLEY (April 2022), https://www.morganstanley.com/ideas/global-ecommerce-growth-forecast-2022.

 [ISSN 2581-5369]

help of the digitization of business practices. E-commerce has generated profits without borders, streamline the supply chain, expanded markets, and reached customers seamlessly. The rise of e-commerce has been attributed to the advantages it has to offer like the convenience to buy on preferred choices, saving time, reading reviews, and comparing products in the comfort of the home. It gives speedy access to the products over multiple websites and has a wide availability of products over domestic and international sales. Furthermore, it has also paved the way for startups, micro, small, and medium enterprises (MSMEs) by lowering their cost and giving them the initial boost to expand and generate profits. The intense competition to capture e-commerce between the big giants has contributed immensely to the speedy delivery of products, inventory management, fast returns, and refunds, lowering cost, and improving efficiency, thereby increasing customer satisfaction and loyalty, and the seamless cycle of e-commerce shopping.

The digitization of business practices has generated data that is considered the oil of the 21st century. The data generated by customers on online shopping has provided valuable insights into behaviors and patterns to the corporations, which in turn are analyzed by them to increase their sales, secure online payments, genius marketing, and retailing strategies, target a particular set of customers, enhanced data-driven decisions, and predict trends, forecasts, and demands[3]. As much as e-commerce has increased, it has also carried a number of legal challenges relating to personal data and consumer protection which need to be addressed[4]. This study intends to provide a comprehensive study of laws and challenges in e-commerce in two major aspects, that is personal data and consumer protection of individuals using e-commerce.

II. PERSONAL DATA PROTECTION, AND E-COMMERCE

"Personal data is any data about an individual who is identifiable by or in relation to such data"[5]. As per the European regulation[6] on the protection of personal data, the words or terminology of 'personal data' holds the key importance in implementing GDPR, then only the processing of personal data applies to GDPR. It is pertinent to note that the mechanism of data protection and the right to privacy are inextricably linked. Data protection is an act of making rules and regulations which protect the sensitive and personal data of individuals, minimize privacy violations, and gives rights to data personal. Violation of data protection makes the data fiduciary, and data processor liable for infringing the rights of individuals and abandoning their

[3] Talend-a qlick company,7 ways big data is changing e-commerce, TALEND A QLICK COMPANY, (2022), https://www.talend.com/resources/big-data-ecommerce.
[4] Adelola, Tiwalade ET. AL, Privacy and Data Protection in E-commerce in Developing Nations: Evaluation of Different Data Protection Approaches, CORE UK, 1, 1-2, (2021).
[5] The Digital Data Protection Bill, 2022, §13.
[6] General Data Protection Regulation, 2018, A4(1).

 [ISSN 2581-5369]

duties. Whereas Personal data is information on the identification and traits of individuals which includes biometric identification, date of birth, etc., or in other words, personal data is a piece of information that is used to identify with some degree of accuracy, a living person. It's pertinent to note that its immaterial from whom personal data is collected.

The supreme court then in the landmark case[7], which changed the Indian scenario, declared the right to privacy as a fundamental right under Article 21 of the Indian constitution. Buying goods and services online has changed the landscape by providing ease and multiple choice to consumers, but also resulted in a number of legal challenges and reliance issues, which pose significant challenges to organizations that engage in electronic commerce. with the massive amounts of data accessible to e-commerce entities. Many online businesses use the personal information of their customers to provide the best possible services as per the preference of the consumers and also gauge their shares of profits. The most significant barriers to the growth of online commerce continue to be privacy concerns and a lack of trust. The Internet industry is based on the trust between e-commerce entities and customers. If consumers feel insecure or face a slew of challenges, their rights protected by the constitutions and relevant statutes are infringed around the world, which has led to enact legislation to protect citizen privacy and corporation information around the world. "The law of data protection around the world are GDPR, the California consumer protection Act (CCPA), Brazil's Lei Geral de Proteção de Dados (LGDP), Personal Information Protection and Electronic Documents Act (PIPEDA), and the UK GDPR"[8]. In India, the recent developments are the PDB Bill, 2019 and, DPDP Bill, 2022 which compacts with data protection.

The Act which deals with personal data and is currently enforced is the IT Act, 2000 which has four sections that talk about the protection of data, 1) Section 43 (a) protects against unauthorized computer system access by imposing a heavy penalty and it applies to unauthorized data downloading, extraction, and copying. This section's clause "c" levies a sanction for the unapproved introduction of harmful substances or virus software. Punishments for encouraging unapproved access are outlined in clause "g". 2) Computer source code is incorporated in Section 65(b). Anyone who knowingly or intentionally conceals, destroys, alters or causes another to do so faces imprisonment or a fine for tampering with a computer source document. 3) Under Section 66 there is anti-hacking protection. This section defines hacking as any action taken with the intent to harm another person without their consent, or with the

[7] Puttaswamy vs Union of India., (2017) 10 SCC 1.
[8] Thales-building a future we can trust, Beyond GDPR: data Protection around the world' 2021, THALES GROUP (May 10, 2021), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world.

 [ISSN 2581-5369]

knowledge that such harm will be done, and requiring the destruction, deletion, alteration, or reduction in value and utility of information stored in a computer resource. This section imposes a three-year prison sentence. 4) Section 72 (d) protects against breaches of data confidentiality and privacy. According to this, whosoever maybe after being granted powers under the statute and IT rules, divulge important information to another party to secure access to it, shall be punished with imprisonment and a fine.

The information technology rules[9] mandate the body corporate to provide a rational safety precautions and uses, the objective of storing and its utilization, transparent and open statement of its rules and guidelines, types of data obtained, dissemination of details including sensitive data (Information regarding an individual's indigenous background or racial origin, views on the nations ‘s politics, religious or ideological convictions, affiliation with a union, and specifics about their physical and sexual well-being are all considered sensitive data.). The IT rules[10] laid down the procedure for the collection of information by the corporations, the data provider's prior consent is mandatory and must be sought when the corporations want to obtain or obtain personal sensitive data. Furthermore, a corporation cannot store or retain sensitive personal information on their whims and fancies but it must be only stored for which the corporation seems necessary. It’s pertinent to note that as per the rules, the required information on data personal must be used only as per the law to make obtaining legitimate or as per the requirement by the enforced laws of the state. Lastly, one cannot forget that only legitimate and essential purposes may justify the obtaining of personal sensitive data as per the rules.

The DPDP Bill of 2022 intends to develop new regulations on data protection in India, which outline the management of digital data for corporations and respects the data protection rights of citizens. The new bill weighs heavily on compliance with the duties of data handlers, and covers the rights of subjects, provides penalties for not following the provisions mentioned in the bill. The DPDP Bill regulates one of the main aspects of data protection that is; the processing of personal data by the fiduciaries, now it’s immaterial from where the data is obtained, it can be gathered manually or via the internet and subsequently converted into electronic or computer-related form. Processing of data can be in a number of forms, the bill covers both non-automated personal data and offline personal data processing, but the processing for domestic or personal use is not covered by the DPDP Bill. The bill excludes from its ambit the personal information of those persons who are found to be in the record of the data fiduciaries for at least a minimum of hundred years. Furthermore, the bill establishes the

[9] IT (Reasonable Security Practices and Sensitive Personal Information) Rules, 2011, R4.
[10] IT (Reasonable Security Practices and Sensitive Personal Information), Rules, 2011, R5.

 [ISSN 2581-5369]

obligations of data fiduciaries and significant data fiduciaries under chapters II and III respectively. The drawback of the Bill is that it has not clearly forbidden cross-border data transfers or specify particular compliance standards that must be met when moving personal data outside of India (such as doing transfer impact analyses or adhering to standard contractual contracts). Additionally, the bill guarantees data subjects' rights to disclosure, rectification, and erasure, as well as their right to a grievance procedure and their right to be nominated[11].

With the exponential growth in data processing and the increasing potential for breaches, it has become essential to establish stringent regulations and hold data fiduciaries and processors accountable for safeguarding personal information. The DPDP Bill recognizes the critical importance of reasonable security safeguards to prevent personal data breaches. Data fiduciaries and data processors are entrusted with the responsibility of protecting this data. Therefore, failure to institute appropriate security measures would face severe consequences. A substantial fine of 25 crore Indian Rupees is imposed to ensure that organizations take data protection seriously, In the event of a data breach, prompt and transparent communication is vital. Failure to notify the appropriate authorities, such as the Board and the data principal, compounds the gravity of the offense. The DPDP Bill stipulates a fine of 2 lakh Indian Rupees to ensure that data fiduciaries and processors uphold their obligation to report data breaches promptly and effectively. Safeguarding the privacy of children's data is a particular area of concern. The DPDP Bill acknowledges this and imposes fines for any failure to fulfill obligations in processing children's data. Data principals also have responsibilities under the DPDP Bill. They must fulfill their obligations in safeguarding their personal data to ensure overall data protection. Failure to perform these duties could result in a fine of 10,000 Indian Rupees. To ensure fairness in assessing fines, the DPDP Bill establishes a cap of Rs. 500 crores per violation. This provision prevents excessive penalties and promotes proportionality[12]. Additionally, individuals who face fines are granted a fair chance to respond, allowing them to present their case and address any misunderstandings or mitigating circumstances[13].

Personal data protection possesses a number of challenges including a lack of trust in the e-commerce entities and their software securities, counterfeiting sites, ransomware, malware[14], fraudulent access to crucial data, breach of information, consent, and transparency,

[11] The Digital Personal Data Protection Bill, 2022, §10, 13, 14, 15.
[12] Securiti ai, An Overview of India's Digital Personal Data Protection Bill 2022, SECURITY.AI, accessed 13th May 2023, 9:45 AM, https://securiti.ai/india-digital-personal-data-protection-bill-pdpb-2022/.
[13] The Digital Personal Data Protection Bill, 2022, §20.
[14] Shoshte Dr. Raj A, A study of data protection and implications for e-commerce, 2 Vol Issue 3. IJARIIE 142, 3, (2017).

 [ISSN 2581-5369]

Jurisdictional issues, and illegal data mining.

III. CONSUMER PROTECTION AND E-COMMERCE

Consumer protection makes sure that clients have access to effective dispute-resolution procedures and are capable of making informed decisions regarding their options. Consumer protection is the process of educating, organizing, and advocating on behalf of consumers in order to defend their interests and well-being from subpar products, dangerous products, and misleading advertisements. Consumer protection is of paramount importance to ensure that consumers are shielded from detrimental commercial practices. The requirement that consumers understand their rights and are equipped to assert them assertively is as important. In[15], the court's explanation of the law highlights the goal of consumer protection, which is to avoid exploitation and stop misconduct. Consumer protection can be effectively sustained by the deployment of strong measures and active participation from all stakeholders, encouraging fair and ethical company behavior while defending the interests of consumers.

The UN has established standard guidelines[16] that emphasize the value of preserving consumer rights and has acknowledged the necessity of consumer protection. These recommendations highlight seven fundamental consumer protection rights that are essential for the welfare and self-determination of people everywhere. The right to be shielded from goods, methods of production, and services that endanger life or health. The information that consumers need to make informed decisions about the goods and services they want to buy should be accurate and transparent and the right to information and the availability of data necessary to make informed decisions are the third right recognized by the UN. The freedom to make choices. The freedom to speak up and have consumer interests reflected when decisions are being made. The right to remedy to be compensated fairly for legitimate.

Consumer protection has received widespread attention, with laws in many nations, including India, recognizing the importance of preserving basic consumer rights. India adopted the Consumer Protection Act in 1986 in accordance with the (UNGCP), with the goal of promoting and safeguarding consumers' rights in accordance with global norms[17], by granting specific rights including the right to safety and information, the right to choose and be heard, the right to seek remedy, and the right to consumer education[18], the Consumer Protection Act of 1986

[15] Raghubir Singh v. Thakurin Sukhraj Kuar, AIR 1939 SC 96.
[16] General Assembly resolution 70/186, United Nations guidelines for consumer protection, E/1999/INF/2/Add.2 (22 December 2015), available from https://unctad.org/system/files/official-document/ares70d186_en.pdf.
[17] Ibid, n15.
[18] The consumer protection Act, 1986, §6. No. 68, Acts of Parliament, 1986 (India).

 [ISSN 2581-5369]

aimed to give consumers more authority. In the Indian context, these regulations represented a substantial step towards safeguarding consumer rights. The statute, however, failed to clearly recognize and safeguard the right to the satisfaction of one's fundamental needs, which include necessities like enough food, clothing, housing, and medical treatment. The right to a healthy environment, which has received significant global attention in recent years, is also not adequately addressed by the act. As customers' awareness of environmental issues grows, it is crucial to shield them from products, business practices, and services that are environmentally harmful. But the act fails to adequately and effectively satisfy two rights that are acknowledged on an international level that is the right to the satisfaction of basic needs and the right to a healthy environment It is important to understand that while the Consumer Protection Act of 1986 offers a procedural mechanism for consumer protection, it does not establish any particular rights or obligations. Instead, it emphasizes a comprehensive and all-inclusive strategy for consumer protection. Although this strategy has advantages, it is required to modify the law to reflect the changing consumer landscape and effectively address new issues[19].

An important step in enabling e-commerce in India was taken with the passage of the Information Technology Act of 2000. The act's provisions do not particularly target consumer protection in the digital sphere, despite the fact that it was intended to encourage internet commerce. Although the statute has a few measures that address consumer protection. The Information Technology Act's Section 10A essentially recognizes contracts entered into electronically without detailing the specific clauses necessary to protect the interests of consumers. Customers are now exposed to various hazards and dishonest practices that could occur in online transactions due to this overlook. Consumers are left to traverse the digital market without proper protection if there are no defined rules and criteria. Additionally, business entities are required by Section 43-A of the act to make restitution to anybody harmed by the loss of personal or sensitive data. This clause, however, only requires compensation when people can show both wrongful loss and unlawful gain. Although this clause recognizes the value of data protection and privacy, it lays the burden of proof on the customer, making it difficult for them to pursue remedies in situations where data is compromised or misused. Enhancing the Information Technology Act's requirements is necessary to protect consumers in e-commerce transactions. In order to protect consumers, there is a need to first construct thorough and lucid clauses in electronic contracts. The act should also have clauses that require corporate entities to take proactive steps to secure personal information. Additionally, it would

[19] Rajiv Khare ET. AL, E-commerce and Consumer Protection: A critical Analysis of Legal Regulations, Vol 1. IJCLP 55, 69-71, (2021).

 [ISSN 2581-5369]

be advantageous to create a specific regulatory agency or body to supervise consumer protection in e-commerce transactions. This organization might be in charge of keeping an eye on and enforcing adherence to consumer protection laws.

Section 66 of the Information Technology Act was added to tackle offenses related to hacking. Moreover, Section 66 only provides a remedy if it can be demonstrated that the damage is being done dishonestly or fraudulently. This means that there is no legal recourse if the harm is caused by an autonomously assisted process or by using other automated methods. The increased sophistication of hacking techniques, including the use of automated systems, artificial intelligence, and bots, is not addressed by this limitation[20]. Additionally, specific consumer protection issues in e-commerce are not specifically addressed under the Information Technology Act. Although the legislation creates a legal foundation for electronic transactions, it is devoid of provisions that address the particular difficulties customers confront when making purchases online. This covers things like dishonest business practices, deceptive marketing, unsafe payment processors, worries about data protection, and conflicts related to online purchases[21]. The lack of concrete solutions to these problems erodes customer confidence and trust in the online economy.

The Consumer Protection Act of 2019, provides six rights to consumers[22] and also defines the term 'unfair trade practices[23], including producing fake goods or rendering subpar services, not providing cash receipts or invoices for purchased goods or services, declining returns or withdrawals of goods or services, neglecting to reimburse the buyer for the payment made, and also revealing the personal information of the consumer. The Central Consumer Protection Authority is established by the new Act in order to combat misleading advertising and unfair corporate practices that affect the public interest. This organization is in charge of policing and monitoring e-commerce operations in order to protect customers. The authority works to safeguard consumers from dishonest business practices by proactively addressing concerns like deceptive marketing, poor product quality, and unfair pricing. The most notable change brought about by the new Act is certainly the inclusion of e-commerce under the purview of consumer protection. The law recognizes the increasing importance of digital transactions by defining e-commerce specifically in Section 2(16). This acknowledgment underlines the necessity of providing customers who make purchases and conduct transactions online with legal

[20] Ibid, n18.
[21] Kalia, P. ET. EL, Information Technology Act in India: e-Commerce Value Chain Analysis, NTUT JIPLM 55, 61-62, (2017).
[22] Consumer Protection Act, 2019, § 2(9), No.35, Acts of parliament, 2019 (India).
[23] Consumer Protection Act, 2019, § 2(47), No.35, Acts of parliament, 2019 (India).

 [ISSN 2581-5369]

protections. Customers now have legal options against e-commerce platforms that breach their rights as a result, resulting in a more secure and dependable online marketplace. By including the idea of product liability, the Act recognizes the particular difficulties faced by consumers in the digital sphere. The prevalence of product flaws and poor service has increased with the growth of e-commerce. With the implementation of this new clause, producers and service providers are now responsible for any harm done to consumers or their property as a result of subpar goods or subpar services. The Act assures that consumers won't be defenseless in the face of damage brought on by the goods or services they buy online by placing the burden of compensating on the appropriate parties.[24] Additionally, the terms "product liability action"[25] and "product manufacturer"[26] are covered by this Act.

The e-commerce protection Act of 2019 provides the rigorous consumer protection framework of the new Act and serves as the foundation for the rules[27]. The date when the E-Commerce Rules comes into force was beneficial given the limitations on consumers' freedom of movement and dependence on online shopping platforms and websites during the corona pandemic[28]. Unquestionably, the grievance resolution mechanism in the rules is a well-balanced step towards retaining market neutrality in e-commerce, more transparency, an impressive harmony between the market commitments made by sellers and e-commerce companies, and stiffer fines. The new regulations mandating the appointment of a consumer grievance redress officer, nodal contact person, or an alternative senior appointed official, along with the duty to provide thorough information and prompt resolution of complaints, mark a fundamental shift in favor of consumers in the ever-expanding world of e-commerce. The regulations enable effective communication and guarantee timely attention to concerns by designating responsible personnel within e-commerce enterprises to manage customer complaints. It promotes accountability and openness to acknowledge customer complaints within 48 hours with a specific ticket number, giving them concrete proof that their issues are being addressed. The increased responsiveness and accountability of e-commerce platforms increases consumer confidence in them Notwithstanding an e-commerce company's return policy, processing refund requests quickly is a big step in the right direction for customer happiness. The return, refund, and exchange policies of the products that a customer is about to purchase must be disclosed to them. E-commerce businesses build a foundation of trust and dependability by providing clear

[24] Consumer Protection Act, 2019, § 2(34), No.35, Acts of parliament, 2019 (India).
[25] Consumer Protection Act, 2019, § 82, No.35, Acts of parliament, 2019 (India).
[26] Consumer Protection Act, 2019, §84, No.35, Acts of parliament, 2019 (India).
[27] Consumer Protection (E-Commerce) Rules, 2020.
[28] Rani Adgulwar, Consumer Protection and E-commerce in India, Vol 18 PAL. ARCHS JOURNALS, 990, 994 (2021).

 [ISSN 2581-5369]

disclosure of warranty and guarantee information, delivery schedules, payment collecting systems, and dispute resolution procedures. By requiring the disclosure of crucial product information, the regulations emphasize consumer protection even more. Customers have a right to important details about the goods they want to buy, including the nation of origin[29]. The regulation prohibiting price manipulation function as a strong deterrent to unethical behavior in the e-commerce sector. Consumers are shielded against inflated or deceptive pricing practices by the express restriction on manipulating prices for profit[30]. This protection makes sure that customers are not the target of misleading practices, allowing them to base their purchases on fair and transparent pricing.

For an online consumer, e-commerce presents a number of barriers including but not limited to, Unfair trade practices and misleading advertisements, E-commerce offers made by anonymous traders, Identity thefts and frauds, Long and tedious refund procedures, Absence and lack of seller's information, delivery and logistics issues, difficulty in resolving disputes, limited redressed options, lack of physical presence of e-commerce entities, and, fraudulent marketing tactics.

IV. CONCLUSION

Personal data and consumer protection play a crucial role in making e-commerce sustainable by contributing to making e-commerce secure and trustworthy. Although, the fact that there is no law in India on data protection. The DPDP bill, of s2022 tries to safeguard Indian citizens' personal data and covers numerous topics, including data processing, consent, data localization, and the creation of an agency that regulates and supervise laws related to data Protection. The measure places a strong emphasis on the requirement that organizations handle personal data with consent, accountability, and transparency. It also acknowledges the significance of cross-border data transfers and suggests safeguards for them. Consumer protection laws serve a significant part in the expansion of e-commerce by incorporating aspects like prohibiting unfair trade practices.

The 2019 consumer protection act lays out the framework and guiding principles for safeguarding consumers' rights during online purchases. It highlights the significance of ethical business conduct, open information sharing, grievance procedures, and data privacy. The rules encourage responsible behavior by platforms and sellers in order to increase customer trust and

[29] Consumer Protection Act, 2019, §5, No.35, Acts of parliament, 2019 (India).
[30] Sarin, Sarthak and Govinda Toshniwal, An Overview Of The Implications Of Consumer Protection Rules For Relevant Stakeholders, INC 42, 1 November 2020, < https://inc42.com/resources/an-overview-of-consumer-protection-e-commerce-rules/.

confidence in online shopping. The e-Commerce Rules 2020" concentrate on avoiding unfair business practices, guaranteeing pricing transparency, combating counterfeit goods, improving consumer complaint redressed channels, and fostering competition and market fairness.

To overcome the challenges in e-commerce on consumer and personal data protection, e-commerce entities must implement strong privacy policies and practices, comply with all applicable data protection laws, obtain users' explicit consent, ensure secure data storage and transmission, carry out privacy impact analyses, and establish precise procedures for data breach management and response. To maintain compliance and safeguard customer data in e-commerce operations, collaboration with legal professionals and frequent monitoring of legislative developments are essential.

*****

 [ISSN 2581-5369]