SHODH SAMAGAM

ISSN : 2581-6918 (Online), 2582-1792 (PRINT)

Role of different Laws for Regulations of E-commerce in India: Challenges and Reforms

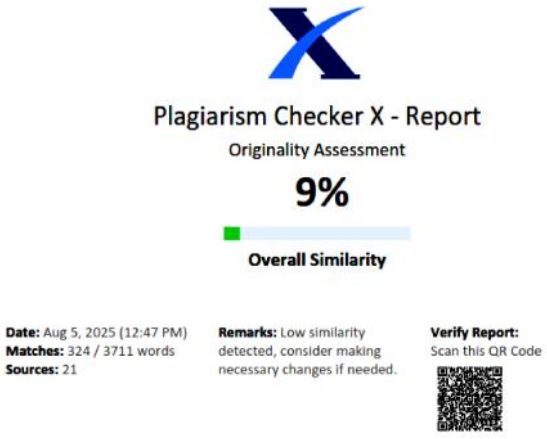
Mukta Verma, Ph.D., Department of Law
University of Allahabad, Prayagraj, Uttar Pradesh, INDIA

ORIGINAL ARTICLE

Author
Mukta Verma, Ph.D.
E-mail : mktverma6@gmail.com

shodhsamagam1@gmail.com

Received on : 03/06/2025
Revised on : 04/08/2025
Accepted on : 13/08/2025
Overall Similarity : 09% on 05/08/2025



ABSTRACT

E-commerce in India has revolutionized the way consumers and businesses interact, driven by rapid digital adoption and mobile internet expansion. However, the country's existing legal and regulatory framework has struggled to keep pace with this exponential growth, leading to significant challenges in governing online trade effectively. This article critically examines the current legal architecture governing e-commerce in India, which is characterized by a fragmented patchwork of laws including the Information Technology Act, Consumer Protection Act, Competition Act and sector-specific regulations like data privacy and foreign investment norms. While these laws provide foundational protections-such as validating electronic contracts, safeguarding consumer rights, regulating anti-competitive conduct, and protecting personal data their scope remains limited and enforcement inconsistent. Key challenges addressed include ambiguity over platform liability where marketplaces exert operational control, complexities in cross-border jurisdiction and enforcement, widespread consumer disempowerment due to asymmetrical bargaining power and opaque standard contracts, proliferation of fake reviews and misleading advertising, and regulatory overlaps among multiple authorities that create compliance hurdles. The article also highlights the critical gap in data protection that persisted until the enactment of the Digital Personal Data Protection Act, 2023, which finally brings a structured framework to govern personal data processed by e-commerce entities. To build a more robust, transparent and accountable ecosystem, the article proposes a suite

of reforms including the enactment of a harmonized, sector-specific e-commerce law that integrates contract, consumer, competition, and data laws calibrated liability norms that align marketplace responsibility with actual control, scalable, technology-enabled online dispute resolution systems to enhance consumer access to justice and stronger international cooperation through bilateral digital trade agreements to address cross-border legal challenges. It advocates for algorithmic transparency and regulatory oversight of AI-driven pricing and recommendations to uphold fairness, and calls for statutory recognition of advertising standards to combat deceptive marketing. By addressing these multifaceted legal issues through coherent reforms, India can foster a fair, innovative and trustworthy e-commerce environment that benefits consumers, sellers and the economy alike.

KEY WORDS

E-commerce, Contract, Competition, Data Privacy, Information Technology.

Legal Framework Governing E-Commerce in India

India does not have a singular comprehensive e-commerce law. Instead, a patchwork of legislations, rules and guidelines regulate various aspects of e-commerce:

1. **The Information Technology Act, 2000:** The Information Technology Act, 2000 (IT Act) serves as the backbone of India's digital legal framework, giving lawful recognition to electronic records and digital signatures, thereby enabling the legitimacy of online transactions and digital commerce. By explicitly validating electronic contracts under Sections 4 to 10, the Act ensures that contracts formed through electronic means such as emails, clickwrap agreements, or digital platforms carry the same enforceability as traditional paper-based contracts. This recognition is crucial in a digital marketplace where parties often never meet physically. Moreover, the IT Act actively addresses a range of cyber offences, including hacking, data theft, identity fraud, and phishing, thus protecting users, consumers, and businesses operating online. In doing so, it not only facilitates trust in digital commerce but also imposes a legal obligation on intermediaries, platforms, and users to adopt reasonable security practices. As technology continues to reshape commerce, the IT Act remains central to upholding legal certainty, consumer confidence and digital accountability.[1]
2. **The Consumer Protection Act, 2019 (CPA 2019):** The Consumer Protection Act, 2019 (CPA 2019) marks a transformative shift in Indian consumer law by expressly extending its scope to cover e-commerce transactions, thereby recognizing the realities of modern digital commerce. For the first time, consumers engaging in online purchases-whether through websites, apps, or digital marketplaces-receive statutory protection equal to those transacting offline. The Act empowers them by granting rights against unfair trade practices, defective goods, and deficient services offered through digital platforms. It also imposes clear legal obligations on e-commerce entities, including mandatory disclosures regarding return policies, refund procedures, payment methods and customer care details. These requirements ensure transparency and reduce information asymmetry, which often disadvantages online buyers.

   The Consumer Protection (E-Commerce) Rules, 2020 further enforce these protections by laying down specific compliance standards for both marketplace and inventory-based models, including the appointment of grievance officers and timelines for resolution of complaints. Through these provisions, the law not only enhances consumer trust in online commerce but also holds e-commerce operators accountable for fair and ethical business conduct.[2]
3. **Contract Law and The Sale of Goods Act:** Standard e-commerce contracts, though formed digitally, are legally binding and governed by the Indian Contract Act, 1872, which lays down the fundamental principles for the formation and enforcement of contracts in India. All essential elements-offer, acceptance, lawful consideration, intention to create legal relations and free consent apply equally to

contracts formed over websites, apps, or digital communication platforms. For instance, when a consumer clicks "place order," it constitutes an acceptance of the seller's offer, creating a binding agreement. These digital interactions, while informal in appearance, are enforceable under the law if they satisfy the statutory requirements of contract formation.

Additionally, the Sale of Goods Act, 1930 supplements this framework by defining the rights and liabilities of parties in online sale transactions, particularly with respect to delivery timelines, transfer of ownership, warranties, and fitness of goods. If a seller fails to deliver the product as promised, or if the product is defective or not as described, legal remedies under the Sale of Goods Act become available. Together, these laws ensure that consumers engaging in e-commerce are afforded the same level of legal protection as in traditional transactions, thereby reinforcing trust and predictability in digital marketplaces.[3]

4. **The Competition Act, 2002:** The Competition Commission of India (CCI) plays a pivotal role in safeguarding fair competition within the rapidly expanding e-commerce sector by scrutinizing and regulating anti-competitive practices commonly observed on digital platforms. These include strategies such as predatory pricing, where goods are sold below cost to eliminate competition, deep discounting, which distorts market equilibrium and exclusive supply or partnership arrangements, which restrict market access for other sellers and limit consumer choice. The CCI, acting under the Competition Act, 2002, actively investigates allegations of abuse of dominant position and practices that amount to preferential treatment of certain sellers often linked to affiliated or private label vendors by major e-commerce platforms. These investigations are crucial, as they address concerns that dominant platforms may leverage their position to tilt the market unfairly, manipulate search algorithms, or control pricing, thereby harming smaller sellers and stifling competition. Through such regulatory oversight, the CCI aims not only to ensure a level playing field but also to promote innovation, consumer welfare, and market integrity in the digital commerce ecosystem.[4]

5. **Data Protection and Privacy Laws:** At present, data protection in India is primarily governed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, framed under the IT Act, 2000. These Rules impose basic obligations on entities handling sensitive personal data such as financial details, passwords and health records to implement reasonable security practices and obtain consent before disclosure.

   However, in the absence of a comprehensive and dedicated personal data protection law, these provisions remained limited in scope, lacked robust enforcement mechanisms and failed to address the complexities of modern digital data ecosystems. Recognizing these gaps, the Digital Personal Data Protection Act, 2023 was enacted to establish a structured, rights-based framework for the protection of personal data. The Act introduces key concepts such as data principals (individuals) and data fiduciaries (entities processing data), and imposes strict compliance obligations on the latter especially on significant data fiduciaries, such as large e-commerce platforms that collect, store, and process vast quantities of consumer data. These obligations include ensuring data minimization, obtaining clear and informed consent, maintaining transparency in data usage, and allowing individuals to access, correct, or erase their data. With this legislation, India has taken a major step toward aligning its data protection regime with global standards, aiming to build consumer trust and accountability in the digital economy.[5]

6. **FEMA and FDI Policies:** Foreign Direct Investment (FDI) in the Indian e-commerce sector is regulated not through a standalone statute, but via a series of Press Notes issued by the Department for Promotion of Industry and Internal Trade (DPIIT) under the umbrella of the Foreign Exchange Management Act, 1999 (FEMA). These Press Notes define the scope, structure and permissible limits of foreign investment in e-commerce. A crucial legal distinction is drawn between two operational models: inventory-based and marketplace-based e-commerce. Under current policy, FDI is strictly prohibited in multi-brand

inventory-based e-commerce, where the platform owns and sells goods directly to consumers, thereby preventing foreign-funded entities from engaging in direct retail. Conversely, 100% FDI is permitted through the automatic route in marketplace models, where the platform merely acts as a facilitator or intermediary between third-party sellers and consumers.

However, this permission comes with stringent compliance conditions, such as non-involvement in pricing, prohibition on ownership of inventory by the platform or its group companies, and the requirement to offer a level playing field to all sellers. These regulations aim to balance the inflow of foreign capital with the protection of domestic retailers, prevent monopolistic practices, and ensure that the marketplace model remains a neutral digital facilitator rather than a disguised inventory player.[6]

Key Legal Challenges in the E-Commerce Sector

Despite these legislations, several legal challenges remain unaddressed or inadequately regulated:

1. **Data Privacy and Cross-Border Transfers:** Most e-commerce platforms, by the very nature of their operations, routinely collect and process vast volumes of personal and behavioural data including browsing history, purchase patterns, location information, payment credentials and preferences of users. Prior to the enactment of the Digital Personal Data Protection Act, 2023, India lacked a comprehensive legal framework to regulate such data processing activities, leading to significant concerns over unregulated surveillance, profiling of users, unauthorized sharing with third parties, and a general erosion of informational privacy. This legal vacuum enabled platforms to engage in opaque data practices without adequate oversight or accountability.

   The issue was further complicated by cross-border data transfers, wherein personal data was often stored or processed in foreign jurisdictions that did not offer data protection standards equivalent to those expected under Indian constitutional values, particularly the right to privacy recognized in Justice K.S. Puttaswamy v. Union of India. Such transfers increased the risk of data misuse, loss of regulatory control, and denial of legal remedies to Indian consumers. The absence of enforceable safeguards in these foreign jurisdictions created a situation where individual privacy was vulnerable to commercial exploitation, state surveillance, and data breaches, highlighting the urgent need for a rights-based, transparent, and accountable data governance regime which the 2023 Act now seeks to address.

2. **Platform Liability and Intermediary Status:** One of the most complex legal challenges in the e-commerce ecosystem is determining the extent of liability of online platforms for the conduct of third-party sellers operating on their marketplaces. Under Section 79 of the Information Technology Act, 2000, e-commerce platforms are typically classified as intermediaries, which grants them a form of conditional safe harbour from liability for content or transactions initiated by users, provided they function merely as facilitators and do not exercise editorial or operational control.

   However, in practice, major platforms like Amazon and Flipkart often play a far more involved role managing logistics, framing return and refund policies, controlling pricing strategies, and even offering private-label products under their own brands. This active involvement raises serious questions about whether such platforms can truly be treated as neutral intermediaries. Their influence over crucial aspects of the transaction lifecycle-such as delivery, inventory storage, customer service, and visibility of products-effectively allows them to shape consumer experience and seller performance, thereby blurring the legal line between a passive intermediary and an active participant in the supply chain. Courts and regulators have begun to scrutinize this model, suggesting that where platforms assume operational control, they should also bear proportionate responsibility for consumer grievances, defective goods, or unfair trade practices. Resolving this issue is key to ensuring accountability, consumer protection, and legal clarity in the digital marketplace.[7]

3. **Jurisdictional Uncertainty:** In the realm of cross-border e-commerce disputes, establishing the appropriate jurisdiction presents a significant legal challenge due to the inherently transnational nature of online transactions. Traditionally, courts have relied on the principle of lex loci contracts, which means the law of the place where the contract was formed, to determine which jurisdiction's laws apply. However, applying this principle becomes complicated in digital commerce because the moment of contract formation is often ambiguous-buyers and sellers may be located in different states or even countries, and the contract may be concluded virtually without any physical presence.

   Moreover, the contract's "place" may be defined by multiple factors, such as the location of the server, the residence of the parties, or the place where acceptance occurs, each leading to conflicting jurisdictional claims. This legal uncertainty is exacerbated by varying consumer protection laws, data privacy regulations, and enforcement mechanisms across jurisdictions, often leaving consumers and sellers without clear legal recourse or protection. Resolving these jurisdictional ambiguities requires innovative legal frameworks, including harmonized international treaties, model laws, or bilateral agreements, which can facilitate predictable dispute resolution, respect sovereign legal boundaries, and uphold consumer rights in the digital marketplace.

4. **Consumer Disempowerment and Asymmetric Bargaining Power:** Despite the existence of robust consumer protection laws, a significant number of consumers remain unaware of their rights or lack the necessary technical knowledge and resources to effectively enforce them in the complex digital marketplace. The widespread use of standard-form contracts, commonly known as clickwrap agreements, further compounds this problem. These contracts, presented as "take-it-or-leave-it" terms during online purchases or platform registrations, are often drafted to heavily favour the interests of e-commerce platforms rather than consumers.

   Such agreements routinely incorporate arbitration clauses that restrict consumers' access to traditional courts, choice of law provisions that select jurisdictions favourable to the platform and limitations on liability that curtail the platform's responsibility for defects or service failures. This creates an imbalance in bargaining power, where consumers must accept these terms without meaningful negotiation, often at the risk of forfeiting important legal remedies. Consequently, the promise of consumer protection in the digital age remains largely theoretical for many users, calling for greater legal awareness initiatives, clearer contract disclosures, and regulatory oversight to ensure that consumer rights are not just enshrined in law but also practically accessible and enforceable.

5. **Fake Reviews and Misleading Advertisements:** The widespread occurrence of fake product reviews and deceptive advertisements poses a serious challenge to the integrity and transparency of the e-commerce ecosystem, yet it remains a largely unregulated and ambiguous area of law. Many online sellers and marketers manipulate consumer perceptions by posting fraudulent reviews or exaggerating product claims, thereby misleading buyers and distorting fair competition. Although the Advertising Standards Council of India (ASCI) has proactively issued self-regulatory guidelines aimed at curbing misleading digital advertising practices including influencer endorsements and fake testimonials-these guidelines are inherently non-binding and lack statutory enforcement power.

   This voluntary compliance framework limits ASCI's ability to impose penalties or compel corrective action, reducing its effectiveness in deterring unethical marketing strategies. Consequently, consumers continue to face risks of deception without a clear legal remedy, while genuine sellers suffer unfair disadvantages. Addressing this gap calls for statutory recognition of ASCI guidelines, enhanced powers for regulatory bodies, and stronger penalties for violations to ensure accountability and restore consumer confidence in digital marketplaces.[8]

6. **Regulatory Overlap and Fragmentation:** The governance of e-commerce in India involves multiple regulatory bodies, including the Competition Commission of India (CCI), Telecom Regulatory Authority

of India (TRAI), Ministry of Electronics and Information Technology (MeitY), Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), and the Ministry of Consumer Affairs. While each regulator has a distinct mandate ranging from competition law and telecommunications to data security, financial transactions, securities regulation, and consumer protection their overlapping jurisdictions in the digital commerce space often lead to regulatory fragmentation and confusion.

E-commerce platforms must navigate a complex maze of compliance requirements, reporting standards and enforcement protocols, which can be inconsistent or even contradictory. This fragmented regulatory landscape increases the compliance burden on businesses, raising operational costs and creating uncertainty regarding which rules apply in specific scenarios. Moreover, the lack of coordination among regulators may result in gaps or duplications in enforcement, ultimately impacting consumer protection and market efficiency. To address these challenges, there is a pressing need for harmonized regulations, inter-agency coordination mechanisms, and a unified digital commerce policy framework that clearly delineates the roles and responsibilities of each regulator, thereby fostering clarity, efficiency and innovation in India's e-commerce sector.

Proposed Reforms and Way Forward

1. **Harmonized E-Commerce Law:** India urgently requires a comprehensive, sector-specific e-commerce legislation that harmoniously integrates key legal domains such as contract law, consumer protection, data privacy, and competition law. Such a unified statute would provide clear definitions of the roles and responsibilities of all stakeholders including platforms, sellers, consumers, and regulators thereby eliminating ambiguity and reducing regulatory overlaps. It should also establish standardized and accessible dispute resolution mechanisms tailored to the digital marketplace, ensuring timely and effective redressal of consumer and commercial grievances. Importantly, this legislation must promote a level playing field by preventing unfair practices and fostering healthy competition, thereby encouraging innovation while safeguarding consumer interests in the rapidly evolving e-commerce environment.[9]
2. **Strengthening Platform Accountability:** The liability of e-commerce marketplaces must be carefully calibrated to correspond with the degree of control they exercise over the transaction process. When platforms go beyond merely facilitating sales and begin to influence critical aspects such as pricing strategies, inventory management, logistics and return policies, they effectively assume a more active role in the commercial relationship. In such scenarios, it is only just and legally sound that these platforms bear proportionate responsibility for ensuring the quality and safety of products sold, as well as for addressing consumer grievances arising from defective or misrepresented goods. This approach acknowledges the evolving nature of digital marketplaces, where platforms often blur the traditional lines between intermediary and principal. By aligning liability with operational control, regulators and courts can ensure that consumers receive effective protection while encouraging platforms to uphold higher standards of accountability and ethical business practices[10].
3. **Unified Consumer Redressal:** An integrated Online Dispute Resolution (ODR) system offers a promising solution to the persistent challenges faced by consumers in accessing timely and affordable justice in e-commerce disputes. By leveraging technology, ODR can streamline grievance redressal, minimize delays and reduce the costs associated with traditional court proceedings. Recognizing this potential, the Department of Consumer Affairs has already launched pilot projects for digital consumer courts aimed at resolving disputes online through virtual hearings, automated case management, and simplified procedures. These initiatives have demonstrated effectiveness in improving access to justice, especially for consumers in remote areas or with limited resources. To maximize their impact, such digital consumer courts and ODR platforms should be scaled up nationwide, creating a unified, user-friendly and efficient dispute resolution ecosystem tailored to the unique needs of the digital economy.[11]

4. **Cross-Border Legal Cooperation:** To effectively tackle the complex challenges of jurisdiction and enforcement in cross-border e-commerce disputes, India must proactively engage in bilateral digital trade agreements with other countries. Such agreements should incorporate clear provisions on mutual legal assistance, enabling cooperation between jurisdictions to investigate and resolve disputes that span national borders. They must also address cross-border data transfers by establishing agreed standards for data privacy and security, ensuring that personal information of consumers is adequately protected regardless of where it is processed. Additionally, these agreements should include robust frameworks for consumer protection, harmonizing regulatory standards to prevent unfair trade practices and providing consumers with reliable mechanisms for redress. By fostering international legal cooperation and regulatory alignment through these targeted digital trade treaties, India can create a more predictable and secure environment for e-commerce, facilitating cross-border commerce while safeguarding the rights of all stakeholders.
5. **Algorithmic Transparency and Ethical AI:** Platforms must disclose the criteria and methodologies underlying personalized pricing, product recommendations, and the ranking of search results to ensure transparency and enable informed consumer decisions. Given the significant impact that algorithmic decision-making has on shaping consumer behaviour and access to products or services, regulatory oversight is essential to prevent discriminatory practices, bias, and unfair manipulation. Such oversight promotes fairness and accountability, ensuring that algorithms operate within ethical boundaries and comply with consumer protection norms. Transparency in algorithmic processes also fosters trust between consumers and digital platforms, making it possible to detect and rectify practices that may otherwise exploit consumer vulnerabilities or distort market competition[12].
6. **Enforceable Advertising Guidelines:** The Advertising Standards Council of India (ASCI) guidelines on influencer advertising and the authenticity of product reviews should be granted statutory recognition to strengthen their enforceability. Incorporating these guidelines into the legal framework specifically under the Consumer Protection Act, 2019 (CPA 2019) would empower regulators to impose penalties for non-compliance, thereby deterring deceptive marketing practices. Such a move would enhance consumer trust by ensuring that endorsements and reviews are transparent, honest, and free from manipulation, aligning with the broader objectives of consumer protection and fair trade in the digital marketplace.[13]

CONCLUSION

India stands at a pivotal moment in shaping the future of its e-commerce landscape by addressing the pressing legal and regulatory challenges that have accompanied its rapid digital transformation. The current fragmented legal framework, though foundational, no longer suffices to protect consumers, promote fair competition, and regulate complex digital interactions effectively. By adopting a comprehensive, sector-specific e-commerce law that unifies diverse aspects such as contract enforcement, consumer rights, data privacy, and competition, India can create a clear, consistent, and balanced legal environment. Holding marketplaces accountable in proportion to their operational control will ensure that consumers receive genuine protection without stifling innovation.

Furthermore, expanding accessible and technology-driven dispute resolution mechanisms will empower consumers to seek redress swiftly and fairly. India's engagement in bilateral digital trade agreements will also be crucial to navigating jurisdictional uncertainties and protecting data and consumer rights across borders. Emphasizing transparency in algorithmic decision-making and enforcing truthful advertising will build greater trust in the digital marketplace. Ultimately, these reforms, driven by a human-centred approach that values fairness, accountability, and inclusivity, will help India foster an e-commerce ecosystem that not only drives economic growth but also respects and empowers every stakeholder in the digital economy.

REFERENCES

1. The Information Technology Act, 2000 (Act 21 of 2000),ss. 4-10.
2. The Consumer Protection (E-Commerce) Rules, 2020, GSR 462(E), Gazette of India (Ministry of Consumer Affairs), July 23, 2020.
3. The Indian Contract Act, 1872; The Sale of Goods Act, 1930.
4. In Re: Alleged Anti-competitive Conduct by Amazon and Flipkart, Suo Moto Case No. 01 of 2020, Competition Commission of India.
5. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
6. DPIIT Press Note No. 2 (2018 Series), Ministry of Commerce and Industry, Government of India.
7. Section 79, IT Act, 2000 and the Intermediary Guidelines (Amendment) Rules, 2023.
8. ASCI Guidelines for Influencer Advertising in Digital Media, April 2021.
9. Ministry of Commerce and Industry, Government of India, *"Draft E-Commerce Policy,"* (2019), https://commerce.gov.in/wp-content/uploads/2020/04/Draft-E-commerce-Policy-2019.pdf and, Justice B.N. Srikrishna Committee Report on Data Protection, *"A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians,"* (2018), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, Accessed on 10/05/2025.
10. Competition Commission of India, *Investigation into Alleged Anti-Competitive Conduct by E-Commerce Entities*, Case No. 01 of 2020, https://www.cci.gov.in/sites/default/files/07_2020_0.pdf and Department of Consumer Affairs, Government of India, *"Guidelines on Liability of E-commerce Platforms,"* (2021), https://consumeraffairs.nic.in/sites/default/files/ecommerce-guidelines.pdf, Accessed on 13/05/2025.
11. NITI Aayog, "ODR: The Future of Dispute Resolution in India", Policy Report (2020).
12. European Commission, *Proposal for a Regulation on Artificial Intelligence*, COM (2021) 206 final, April 21, 2021 and Ministry of Electronics and Information Technology, Government of India, *Draft National Strategy on Artificial Intelligence*, June 2018.
13. Advertising Standards Council of India, *Guidelines for Influencer Advertising in Digital Media*, April 2021, https://ascionline.org/guidelines-for-influencer-advertising/, Accessed on 15/05/2025.

****