Journal of International Commercial Law and Technology

Print ISSN: 1901-8401

Website: https://www.jiclt.com

"The legal liabilities of e-commerce platforms for data breaches and unfair trade practices by third-party sellers"

Article History:

Name of Author:
Anurag Pandey[1], Dinesh Kr. Pandey[2], C K Dwivedi[3], Ashish Shukla[4], Harit Kumar[5]

Affiliation:
[1]-Professor, Department of Business Administration, Pranveer Singh Institute of Technology, Kanpur.
ORCHID ID : 0009-0004-5585-4625
[2]-Professor, Department of Business Administration, Pranveer Singh Institute of Technology, Kanpur.
ORCHID ID : 0000-0002-7792-7774
[3]-Associate Professor, Department of Business Administration, Pranveer Singh Institute of Technology, Kanpur.
ORCHID ID : 0009-0003-0656-0009
[4]-Associate Professor, Department of Business Administration, Pranveer Singh Institute of Technology, Kanpur.
ORCHID ID : 0009-0008-1566-6207
[5]-Professor, Department of Business Administration, Pranveer Singh Institute of Technology, Kanpur
ORCHID ID : 0000-0003-3385-4056

How to cite this article: Anurag Pandey, Dinesh Kr. Pandey, C K Dwivedi, Ashish Shukla,Harit Kumar, "The legal liabilities of e-commerce platforms for data breaches and unfair trade practices by third-party sellers": 1208-1214.

Abstract

With the emergence of online market place, the e-commerce has been growing rapidly. These online market place control many complex legal problems including accountability and liability for any misconduct done by the third-party sellers. This research paper is written to elaborate the legal framework and increasing jurisprudence concerning to the liability

The e-commerce is growing at rapid pace due to the emergence of online market places, which has controlled to complex legal problems with regards to platform accountability or liability for any delinquency by the third-party sellers. This research paper based on the systematic literature review aims to summarize the legal framework and evolving jurisprudence relating to e-commerce platforms' liability for data breaches and unfair trade practices initiating from third-party sellers while studying legal frameworks in key regions, such as the EU's Digital Services Act (DSA), India's Consumer Protection (E-commerce) Rules, and the US's INFORM Consumers Act, emphasising a trend towards greater platform accountability. The key findings of this research paper show a world-wide shift away from the "mere intermediary" Défense, with jurisdictions gradually impose liability based on the knowledge of misconduct, platform's level of active participation, and failure to exercise due diligence and concludes that e- commerce platforms can be held legally responsible for data breaches and unfair trade practices by third-party sellers so the platforms' legal and ethical obligations grow as they take on more active roles in transactions, consumer protection policies, openness and calling for strict adherence to regulations. Although the extent of this liability varies greatly by jurisdiction. The legal frameworks typically strike a balance between safeguarding platforms from third-party content through "safe harbor" provisions and defending consumer rights..

Keywords: e-commerce, platform liability, data breach, third-party sellers, unfair trade practices, intermediary liability, digital services act, consumer protection, online market place

Introduction

The e-commerce ecosystem has evolved with the proliferation of online marketplace platforms that enable third party sellers to access a sizable customer base. While this model enhances consumer choice and promotes economic development, it introduces significant risks. Consumers trust the marketplace's brand, but they often contract with unknown third-party sellers, exposing them to unfair trading, data breaches, and privacy risks. At least 36% of all data breaches originated from third-party compromises in 2024, representing a 6.5% year-over-year increase. There were 3,205 publicly reported data compromises have been seen in 2023, that impacted an estimated 353,027,892 individuals, representing a 78% increase over 2022, Between September 2022 and September 2023, there were over 4,608 data breaches reported in the US, with over 5 billion affected records and 98% of organizations have at least one third-party vendor that has suffered a data breach. In April 2024, Pandabuy, a Chinese e-commerce platform, suffered a data breach compromising the personal information of

approximately 1.3 million users, including names, contact details, order information, and addresses. The average cost of a data breach reached an all-time high in 2024 of $4.88 million, a 10% increase from 2023. Countries are struggling with the question of how much legal responsibility these platforms should have for the sellers' misconduct and unfair practices. Platforms have largely enjoyed the "safe harbor" immunity, which treats them as neutral intermediaries and does not hold them liable for the acts of third parties. There is a shifting balance, however, toward recognizing that many platforms are no longer passive conduits, as recent legislative and judicial developments suggest. Because of these platforms' active roles in advertising, content curation, payment and package processing, they are liable and assume a blurred legal boundary. However, as recent judicial and legislative events indicate, the balance is shifting in favor of acknowledging that many platforms are no longer passive conduits. These platforms are accountable and assume a fuzzy legal boundary due to their active activities in advertising, content selection, payment processing, and package handling.

The rapid growth of e-commerce has given rise to complex legal questions about the platform's accountability for the actions of third-party sellers. Consumers anticipate that platforms will uphold ethical business practices and safeguard their data. However, many platforms operate as "marketplaces" that assert themselves as unreliable middlemen. The main concerns and legal developments influencing the shifting socio-legal landscape of the issue are highlighted in this systematic literature review, which gathers and examines the legal and regulatory scholarship on the liability of e-commerce platforms for data breaches and for third-party sellers' unfair trade practices.

1. Theoretical Framework

This study is based on a number of related legal and economic theories:

2.1. Theory of Intermediary Liability

This theory looks at the online platforms' liability concerning illegal content or the user's actions and to what extent they can be held liable (Rajagopal 2019). This theory's central point is the concept of 'safe harbor' which provides platforms some shield from liability if they comply with some requirements including notice-and-take-down policies (S.S. Rana & Co. n.d). As reported by S.S. Rana & Co. (n.d.), the model aims to investigate the shift from the passive intermediary paradigm to the more engaged intermediary paradigm and the consequences on liability safe harbors will be lost.

2.2. Enterprise Liability Theory:

Even if the particular acts were not expressly approved, enterprise liability makes a company accountable for the deeds of its representatives (Busroh et al., 2025). In the context of e-commerce, where the platform's systems, marketing, and brand are crucial to the transaction, this study applies this theory. According to the framework, platforms should be held accountable for the wrongdoing of third parties since they establish the "enterprise" that permits the harm, particularly when they have a substantial amount of market power (Busroh et al., 2025).

2.3. Theory of Asymmetric Information

According to this economic theory, when one party to a transaction has more or better information than the other, market failures take place (ResearchGate, 2024). Platforms have far more information about sellers, transaction histories, and security flaws than do customers in the context of e-commerce. According to the framework, platforms may underinvest in security and oversight as a result of this information asymmetry, which leads to moral hazard. One way to align platform incentives with consumer welfare is through legal liability (ResearchGate, 2024).

2.4. Consumer Protection Theory

This perspective focuses on protecting consumers from harm, particularly when market power is imbalanced (StockGro, 2025). This framework will analyze how data breaches and unfair trade practices violate fundamental consumer rights to safety, information, and fair dealing. Legal liability is viewed as a necessary tool to enforce these rights and deter platforms from prioritizing profits over consumer well-being (StockGro, 2025).

3. Research Questions

The theoretical framework will be used to guide a systematic literature review addressing the following research questions:

1. Under what conditions are e-commerce platforms held legally liable for data breaches caused by third-party sellers?
2. What legal liabilities do e-commerce platforms face for unfair trade practices committed by third-party sellers on their platforms?
3. How have legal standards for e-commerce intermediary liability evolved in different jurisdictions regarding third-party seller misconduct, moving beyond "mere conduit" to "active participant"?

4. What theoretical justifications exist for extending enterprise liability to e-commerce platforms for data breaches and unfair trade practices, particularly when the platform exercises substantial control over the transaction?

5. How do information asymmetries between platforms, third-party sellers, and consumers impact the determination of legal liability, and how can liability rules be designed to correct for this imbalance?

6. To what extent do existing consumer protection frameworks address the unique challenges of e-commerce, and what theoretical and practical gaps remain concerning data breaches and unfair trade practices?

4. Methods

This research will employ a systematic literature review methodology, following the PSALSAR framework (Protocol, Search, Appraisal, Synthesis, Analysis, Reporting) (Mengist et al., 2020).

A search of electronic databases (e.g., Scopus, Web of Science, HeinOnline, LexisNexis) was conducted using keywords and Boolean operators related to e-commerce, platform liability, third-party sellers, data breaches, and unfair trade practices. The search was limited to peer-reviewed articles, books, and legal analyses published in English. After an initial screening of titles and abstracts, eligible studies were subjected to full-text review. Inclusion criteria focused on studies discussing the legal liabilities of e-commerce platforms for the specified misconduct by third-party sellers.

- Search Strategy: A comprehensive search of academic databases (e.g., Scopus, Web of Science, HeinOnline, LexisNexis), law reviews, and legal analyses will be conducted. The search for relevant literature was conducted across multiple databases, including legal journals, academic repositories, and reputable legal news outlets. The search terms included permutations of: e-commerce platform liability, intermediary liability, marketplace liability, third-party seller, data breach, personal data protection, consumer protection act, unfair trade practices, Communications Decency Act, Digital Services Act, product liability and relevant legal theories.

- Inclusion/Exclusion Criteria: The review will include peer-reviewed journal articles, law articles, book chapters, and reports discussing the legal liabilities of online platforms for misconduct by third-party sellers, covering data privacy and consumer protection issues. Jurisdictional scope includes India, the European Union, and the United States, given their influential legal frameworks. Studies focused exclusively on intellectual property infringement or general contract law, or covering jurisdictions outside the selected scope, were excluded.

- Data Extraction and Synthesis: Data was extracted from included studies using a structured template to capture:

- Legal framework and jurisdiction

- Context of liability (data breach or unfair trade practice)

- Factors influencing platform liability (e.g., knowledge, control, involvement)

- Key judicial precedents or regulatory actions

- Mitigation strategies discussed

The findings were synthesized qualitatively to identify patterns, evolving legal standards, and areas of convergence and divergence across different legal systems.

- Analysis and Reporting: The synthesis will analyze current knowledge, identify theoretical and empirical gaps, and map out the legal evolution of platform liability. The final report will present the findings, discuss their implications for e-commerce regulation, and suggest future research directions.

5. Findings and discussion

5.1 Legal liability for data breaches by third-party sellers

A data breach is the unauthorized exposure or loss of personal information, which can have severe financial and reputational consequences for both consumers and platforms. The legal liability of e-commerce platforms in these situations hinges on their role and responsibilities regarding customer data.

5.1.1 Intermediary immunity vs. active participation

- Traditional intermediary role: Historically, platforms have claimed limited liability for user-provided data under "safe harbor" provisions, like Section 79 of India's IT Act, which grants immunity as long as the platform does not initiate, select, or modify third-party data and exercises due diligence.

- Erosion of immunity: Judicial decisions are increasingly challenging this position. Courts have found that when a platform becomes an "active participant" by providing value-added services—such as payment processing, warehousing, or customer service—it may lose its intermediary protection. This active involvement can imply a duty of care towards customer data.

5.1.2. Data protection regulations and accountability

• India's Digital Personal Data Protection Act (DPDP Act), 2023: This legislation significantly increases the obligations of e-commerce platforms, which are considered "Data Fiduciaries". It mandates obtaining explicit consent, implementing strong security measures, and appointing Data Protection Officers. Critically, platforms must ensure data collected for a specified purpose is deleted when that purpose is no longer served. A breach by a third-party seller could implicate the platform for failure to ensure adequate data protection across its ecosystem.

• EU's Digital Services Act (DSA), 2024: The DSA reinforces consumer safety by imposing stricter obligations on online marketplaces, making them more responsible for the traders they host. Platforms must collect and verify seller information and, if they become aware of an illegal product sale, must inform affected consumers. While platforms are not liable for user misconduct by default, they can be held responsible if they fail to act upon becoming aware of an illegal activity.

• US legal landscape: The US lacks a single, comprehensive federal data protection law, but sector-specific and state laws like the California Consumer Privacy Act (CCPA) govern data handling. The INFORM Consumers Act also increases transparency by requiring marketplaces to collect, verify, and disclose certain information about "high-volume" third-party sellers. While the Communications Decency Act (CDA) generally provides immunity for third-party content, it is less effective in shielding platforms from product liability or data protection claims related to their own conduct.

5.1.3. Negligence and foreseeability

Platforms can be held liable under tort law for negligence, especially if they fail to implement reasonable security practices despite the known risks of breaches. Courts have the authority to determine whether the platform's security protocols were appropriate given the volume and sensitive nature of the data it handled. In the event of a subsequent data breach, a platform that is aware of a seller's prior security concerns but does nothing could be deemed negligent.

Because e-commerce platforms are involved in the collection, processing, and storage of enormous volumes of customer data, legal frameworks around the world are having difficulty holding them responsible for data breaches.

- Intermediary vs. Data Fiduciary: In many jurisdictions, the critical distinction hinges on whether the platform acts purely as an intermediary or as a "data fiduciary". Platforms are directly liable for data breaches and have a greater duty of care as data fiduciaries, whereas their liability as intermediaries is frequently conditional.
- Due diligence obligations: To qualify for legal safeguards as intermediaries, platforms must exercise due diligence as indicated in the Information Technology (Intermediaries Guidelines) Rules, 2011, of India. The safe harbor protections may lapse if the platforms do not observe reasonable security measures.
- Active vs. passive role: One important factor in determining liability is the type of involvement the platform has. A platform is better protected if it is only a passive information channel. Courts are more likely to impose liability, though, if it actively participates, for example, by altering information, managing search results, or offering specific payment processing services.
- Jurisdictional differences: The landscape of international data protection regulations is diverse. While India's Digital Personal Data Protection Act (DPDPA), 2023, has imposed more stringent requirements for data fiduciaries, including e-commerce platforms, requiring transparent data collection practices, robust security measures, and prompt breach notifications, the European Union's GDPR sets a high standard for data protection.

5.2. Legal liability for unfair trade practices by third-party sellers

Selling faulty or fake goods, giving false descriptions, or using dishonest pricing are examples of unfair trade practices (UTPs) committed by third-party sellers. One of the main concerns in consumer protection is the liability of e-commerce platforms for these actions.

5.2.1. Consumer protection regulations

India's 2020 E-commerce Regulations and 2019 Consumer Protection Act: In India, platform immunity was severely undermined by this framework. Important clauses consist of:

- "Fall-back liability": If a seller fails to deliver or the customer suffers a loss, the marketplace may be held liable.
- Transparency: Platforms are required to offer thorough seller information, including contact information, product descriptions, and grievance procedures.
- Prohibition of UTPs: Platforms are expressly forbidden by the rules from engaging in price

manipulation or other UTPs, such as permitting deceptive advertising.

- EU's DSA: The DSA makes marketplaces more responsible for product safety and legality in addition to data security. When illegal products are found, they must take proactive measures to remove them and, in certain situations, warn customers about the risks.

- US consumer laws: UTPs are governed by FTC regulations and state-level consumer protection laws. In the past, the CDA frequently protected platforms from claims of product liability. Nonetheless, some courts have held platforms accountable, particularly in cases where they have substantial control over transactions, like managing fulfillment. By requiring high-volume sellers to disclose, the INFORM Consumers Act also helps reduce UTPs by discouraging the sale of unsafe or counterfeit goods.

5.2.2. Judicial interpretations and control

Courts frequently analyze the level of control a platform exercises over the third-party transaction to determine liability. For instance, if a platform's branding, guarantees, or logistics services lead a consumer to believe the platform is the seller, it may be held liable. Landmark cases have established that platforms can't hide behind a "mere conduit" argument if their actions actively aid or enable unfair practices.

5.2.3. Product liability

The concept of "product liability" has expanded to encompass e-commerce platforms. If a platform is deemed to be in the chain of distribution, it may be held liable for defective products, especially if the third-party seller is located abroad or is difficult to trace. Legal scholars and courts have debated whether platforms should be viewed as sellers for warranty and liability purposes under commercial codes.

Liability for unfair trade practices

Platforms are increasingly being scrutinized for third-party sellers' unfair trade practices, such as selling counterfeit products, publishing fake reviews, and engaging in misleading advertisements.

- Notice and takedown requirements: The "actual knowledge" standard is central to many intermediary liability laws concerning unfair trade practices. Platforms are often required to take down infringing content promptly upon receiving a specific notification from a rights holder. Failure to act can result in secondary or contributory liability.

- Brand infringement: Platforms that is involved or helps the fake products trade may face violations for trademark infringement. The complex legal fights over platform liability to prevent the sale of counterfeits are revealed through litigation, like Tiffany v. eBay.

- Prophylactic filtering: Prophylactic filtering of listings are the types of actions which courts often expect from platforms that have demonstrable control over their listings, even if there is no independent-duty-to-monitor; An important question is the extent of control, such as how products are advertised or ranked.

- · Misleading advertisements and reviews: There are several consumer protection laws against platforms hosting fake reviews or hiking up product prices, such as India's Consumer Protection (E-Commerce) Rules, 2020.

-

- · Fallback liability: Some draft amendments in various jurisdictions suggest a "fallback liability," under which platforms would be liable if sellers are unable or fail to fulfil their obligations. This would impose greater responsibility on the platform for the misconduct of sellers.

- Seller information disclosure: Platforms are already legally obligated to offer consumers information about third-party sellers that is clear and easy to find. This increased level of transparency will allow consumers to make informed choices and save them from having to resort to the manufacturer for a remedy.

7. Conclusion

Instead of broad immunity, a more balanced proposal grounded in platform liability has emerged to redefine e-commerce platforms' liability more flexibly and dynamically in the rapidly evolving legal environment. Quantitative synthesis The systematic review produces a number of key findings:

- Erosion of intermediary immunity: The more that a platform is involved in the transactions it facilitates, the less traction remains for the passive intermediary shield.

- The rise of accountability: Platforms are facing proactive duties with respect to seller verification, transparency, and consumer remedies as a consequence of new regulations deferentially, within India and the EU especially.

- Active control as a liability determinant: Court decisions are more and more linking the extent of active involvement and control by a platform to its legal liability for the misconduct of third parties.

- Greater complexity: Multinational platforms sit within a multi-faceted environment which requires tailored compliance response given the divergent treatment of the issue at the different jurisdictional level.

Dealing with the legal responsibilities of e-commerce platforms as a result of another vendor fraud, abuse or some other regulations in place is highly dependent on the legal system present in that jurisdiction. This decision is also influenced by such factors as the contractual terms of the transaction in question. The moment a court finds a platform to actively intervene and manage the transaction, the platform loses the legality of an intermediate agent. Since the transaction is actively managed by the site, it is strongly advised to the vendors to develop a certain knowledge of the robust management of the security risks more so that the current data management and the customer protection requirements. There is also need of constant tracking of the regulations. Further research can focus on how the legal environment of the transaction is being impacted by the new regulations and technology such as “fallback liability”.

Future studies should concentrate on the application and efficacy of new legislation in holding platforms accountable, such as the EU's DSA and India's DPDP Act. Furthermore, it would be beneficial to conduct research on how platform liability is affected by cutting-edge technologies like artificial intelligence and automated moderation. Lastly, a crucial area of legal scholarship will remain the comparative legal analyses that examine how various jurisdictions handle conflicts between consumer protection laws and intermediary immunity laws.

8. Significance of the Study:

This study is very important both theoretically and practically. By offering a strong framework for comprehending the intricate legal relationships in e-commerce, it theoretically advances the conversation on platform governance. It provides a more complex understanding of platforms' function as market gatekeepers and challenges the traditional perception of them as passive intermediaries. Practically, the findings will provide crucial insights for policymakers, regulators, and legal practitioners grappling with platform accountability. By clarifying the legal basis for platform liability, the research can inform the development of more effective consumer protection and data security regulations in the digital age.

9. Scope for future Research:

Future research could investigate how well such new pieces of legislation, like the EU DSA and India's DPDP act, address the issue of holding platforms accountable. Secondly, research is needed to determine the impact of new technology like artificial intelligence and automated moderation on the platform's liability. In the end, a critical area for scholarly contribution that remains is the comparative legal analysis on what conflicts of consumer protection and intermediation immunity laws are being solved in different jurisdictions.

REFERENCES

1. Agrawal, S. (2023). An analysis of the liability of e-commerce platforms for data breaches in India. JLRJS, 4(1), 1-22. https://jlrjs.com/wp-content/uploads/2023/11/22.-Shivam-Agrawal.pdf
2. B&B Associates LLP. (n.d.). Section 94 Consumer Protection E-Commerce India. Retrieved August 23, 2025, from https://bnblegal.com/article/section-94-consumer-protection-ecommerce-india/
3. Busroh, F. F. et al. (2025). The responsibility of the online marketplace to protect consumer data privacy in E-commerce transactions. ResearchGate. https://www.researchgate.net/publication/387353936_The_Responsibility_of_the_Online_Marketplace_to_Protect_Consumer_Data_Privacy_in_E-commerce_Transactions
4. Data breach. (n.d.). Wikipedia. Retrieved August 23, 2025, from https://en.wikipedia.org/wiki/Data_breach
5. Description of the Systematic Literature Review Method. (n.d.). Technische Universität Berlin. Retrieved August 23, 2025, from https://www.tu.berlin/en/wm/bibliothek/research-teaching/systematic-literature-reviews/description-of-the-systematic-literature-review-method
6. E- Commerce Website and Their Liabilities in India. (2023, February 15). LawBhoomi. Retrieved August 23, 2025, from https://lawbhoomi.com/e-commerce-website-and-their-liabilities-in-india/
7. Jain, A., & Goyal, S. (2023). Liability of online marketplace vis-a-vis trademark infringement: Development across jurisdictions. Taxmann. https://www.taxmann.com/research/company-and-sebi/top-story/105010000000023477/liability-of-online-marketplace-vis-a-vis-trademark-infringement-development-across-jurisdictions-experts-opinion

8. Jain, A., & Gupta, P. (2024). The legal implications of e-commerce in India. Free Law. https://www.freelaw.in/legalarticles/The-Legal-Implications-of-E-commerce-in-India
9. Legal issues in e-commerce and online transactions. (2024, September 22). iPleaders Blog. https://blog.ipleaders.in/legal-issues-in-e-commerce-and-online-transactions/
10. Maheshwari & Co. (2024, August 1). 9 Regulations for setting up an e-commerce business in India. https://www.maheshwariandco.com/blog/understanding-indian-e-commerce-regulations-a-guide-for-foreign-companies/
11. Mengist, W., Soromessa, F., & Legese, G. (2020). Method for conducting systematic literature review and meta-analysis for environmental science research. ScienceDirect, 15(1), 1-13. https://www.sciencedirect.com/science/article/pii/S221501611930353X
12. Mengist, W., Soromessa, F., & Legese, G. (2020). Method for conducting systematic literature review and meta-analysis for environmental science research. ScienceDirect, 15(1), 1-13. https://www.sciencedirect.com/science/article/pii/S221501611930353X
13. Mondaq. (2025, January 15). Navigating DPDPA compliance for e-commerce businesses. https://www.mondaq.com/india/data-protection/1561336/navigating-dpdpa-compliance-for-e-commerce-businesses
14. PSL Chambers. (2020). An overview of the Consumer Protection (E-Commerce) Rules, 2020. https://www.pslchambers.com/psl-release/an-overview-of-the-consumer-protection-e-commerce-rules-2020/
15. Rajagopal, S. (2019). The changing landscape of intermediary liability for e-commerce platforms in India. IJLT, 16(2), 1-28. https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1021&context=ijlt
16.
17. Rajagopal, S. (2019). The changing landscape of intermediary liability for e-commerce platforms in India. IJLT, 16(2), 1-28. https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1021&context=ijlt
18. ResearchGate. (2024, June 5). The determination of "corresponding liability" for the e-commerce platform business. https://www.researchgate.net/publication/381360392_The_determination_of_corresponding_liability_for_the_e-commerce_platform_business
19. Roy, A. & Choudhury, S. (2025). Recalibrating Consumer Rights in the Digital Marketplace: A Critical Analysis of India's E-Commerce Rules. IJLSSS, 7(1), 1-28. https://ijlsss.com/recalibrating-consumer-rights-in-the-digital-marketplace/
20. S.S. Rana & Co. (n.d.). E-Commerce Intermediary Liability India. Retrieved August 23, 2025, from https://ssrana.in/corporate-laws/information-technology-law-india/ecommerce-intermediary-liability-india/
21. Secureframe. (2025). 110+ of the latest data breach statistics [Updated 2025]. https://secureframe.com/blog/data-breach-statistics
22. Sharma, R. (2024, October 22). A summary of consumer protection (e-commerce) rules, 2020. IndiaLaw LLP. https://www.indialaw.in/blog/civil/consumer-protection-e-commerce-rules/
23. Bright defence, (2024, April). Data Breaches That Occurred in April 2024. https://www.brightdefense.com/resources/recent-data-breaches/
24. Sharma, V. (2021). Legal framework for e-commerce in INDIA. IJRPR, 4(6), 1-13. https://ijrpr.com/uploads/V6ISSUE4/IJRPR43043.pdf
25. Sinha, A. (2024). Protecting consumer data in the age of e-commerce: A study of Indian laws and practices. Free Law. https://www.freelaw.in/legalarticles/Protecting-Consumer-Data-in-the-Age-of-E-commerce-A-Study-of-Indian-Laws-and-Practices
26. Maheshwari & Co. (2024, August 1). 9 Regulations for setting up an e-commerce business in India. https://www.maheshwariandco.com/blog/understanding-indian-e-commerce-regulations-a-guide-for-foreign-companies/
27. StockGro. (2025, May 2). Unfair Trade Practices: Definition, Examples, and Legislation. https://www.stockgro.club/blogs/stock-market-101/unfair-trade-practices/
28. Systematic review. (n.d.). Wikipedia. Retrieved August 23, 2025, from https://en.wikipedia.org/wiki/Systematic_review
29. Vats, V. (2023, August 11). How data protection laws impact e-commerce in India. Lloyd Law College. https://www.lloydlawcollege.edu.in/blog/data-protection-laws-impact-ecommerce.html
30. PwC. (2023, August 15). DPDP Act: Impact on E-Commerce and Services Sector.

How to cite this article: Anurag Pandey, Dinesh Kr. Pandey, C K Dwivedi, Ashish Shukla,Harit Kumar, "The legal liabilities of e-commerce platforms for data breaches and unfair trade practices by third-party sellers": 1208-1214.

https://www.pwc.in/blogs/digital-data-protection-act.html