Page 357 - 368

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Emerging Issues in Cross-Border E-Commerce, Data Protection, and Digital Governance: A Review of the Indian Consumer Protection Framework

INDRAJITH N* AND ABINASH MOHANTY**

ABSTRACT

The proliferation of online retail has outpaced the legal and institutional architecture designed to govern it, exposing consumers to risks that are increasingly cross-border, data-intensive, and platform-mediated in nature. This paper undertakes a detailed review of the literature on India's consumer protection framework for e-commerce, principally the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020, to identify emerging issues in cross-border trade, data protection, and digital governance. Drawing on four recent doctrinal and empirical studies, the review traces the statutory evolution from the Consumer Protection Act, 1986 to the 2019 Act, examines the specific provisions governing product liability, marketplace and inventory e-commerce entities, grievance redressal, and penal consequences, and evaluates the operational record of the Central Consumer Protection Authority (CCPA). The review finds that although India has constructed a comparatively comprehensive statutory and institutional apparatus, three structural gaps persist: jurisdictional reach has outpaced enforceability in cross-border disputes; data protection is addressed only derivatively, as a species of unfair trade practice, rather than as a freestanding regulatory domain; and digital governance institutions face unresolved ambiguity in allocating liability across multi-seller marketplace platforms. The paper concludes with a set of recommendations addressing enforcement infrastructure, data-protection integration, marketplace liability clarity, and consumer education.

Keywords: *cross-border e-commerce, data protection, Consumer Protection Act 2019, Consumer Protection (E-Commerce) Rules 2020, product liability*

I. INTRODUCTION

Electronic commerce has moved from a peripheral convenience to a dominant mode of commercial exchange, reshaping how consumers discover, evaluate, and purchase goods and

* Author is a Student at Amity University, Bengaluru, Karnataka, India.
** Author is a Student at Amity University, Bengaluru, Karnataka, India.

services. India illustrates this shift starkly: the domestic e-commerce market is projected to reach US$111.40 billion by 2025, growing at a compound annual growth rate of 19.24% in categories such as grocery and fashion, and India's e-commerce sector has secured ninth rank in cross-border growth globally (Aher & Sable, 2021). Internet connectivity has grown in parallel, with internet connections in India reaching 784.59 million by July 2021 and online shoppers projected to reach 220 million by 2025 (Aher & Sable, 2021). This growth, however, has not been frictionless. Chawla and Kumar (2022) document that international online fraud reports, tracked through the econsumer.gov initiative, rose from roughly 14,800 cases in 2015 to over 40,000 in 2019, with a reported loss exceeding US$151 million in that year alone, and with India ranking third globally in consumer-side fraud complaints and fifth in company-location-based complaints.

Three structural features of contemporary e-commerce generate the governance challenges this paper examines. First, cross-border transactions introduce sellers, warehouses, and payment intermediaries operating outside the consumer's home jurisdiction, complicating both the applicable law and the practical enforceability of any judgment obtained. Second, e-commerce business models are inherently data-intensive: consumer identity, payment credentials, browsing behaviour, and location data are collected, processed, and frequently transferred across borders, creating privacy exposures with only an indirect statutory remedy under current consumer law. Third, the rise of multi-sided marketplace platforms, where the platform itself is neither manufacturer nor seller but an intermediary connecting the two, has generated persistent ambiguity about where liability for consumer harm should rest.

India's legislative response to these pressures has been substantial. The Consumer Protection Act, 1986 was repealed and replaced by the Consumer Protection Act, 2019, which came into force on 20 July 2020 and is supplemented by the Consumer Protection (E-Commerce) Rules, 2020, notified on 23 July 2020 (Chawla & Kumar, 2022; Aher & Sable, 2021). This reform is frequently presented, both in government communications and in parts of the academic literature, as a comprehensive modernisation suited to the digital economy. This review interrogates that claim in detail by synthesising four recent studies, tracing the statutory architecture provision by provision, and asking whether legislative comprehensiveness has, in practice, translated into effective protection against cross-border, data-related, and platform-mediated harms.

II. Statement of the Problem and Research Objectives

Despite a modernised statutory framework, questions remain about whether Indian consumer protection law adequately addresses the transnational and data-driven character of contemporary e-commerce. Sellers frequently operate without a fixed domestic presence; platforms intermediate between numerous third-party sellers without a settled allocation of liability; and personal data flows across borders with limited consumer visibility or control. Tamilmani and Archana (2025) frame this precisely as an open question: whether the existing legal framework under the 2019 Act adequately protects consumers involved in e-commerce transactions, given persistent limitations in consumer awareness, enforcement capacity, and the treatment of evolving digital business models.

This review pursues four objectives: (i) to trace how the statutory and regulatory framework evolved from the 1986 Act to the 2019 Act and its accompanying Rules, with particular attention to provisions relevant to cross-border trade; (ii) to assess how data protection concerns are addressed, whether directly or derivatively, within consumer protection instruments; (iii) to evaluate the institutional record of the CCPA and the marketplace/inventory distinction drawn by the E-Commerce Rules as instruments of digital governance; and (iv) to identify, from the convergence and divergence across the reviewed studies, the specific gaps that ongoing reform should prioritise.

III. Research Methodology

This review adopts a doctrinal and analytical methodology, consistent with the approach used in the primary sources themselves (Tamilmani & Archana, 2025). It relies on four secondary sources selected for their direct engagement with the Consumer Protection Act, 2019 and its E-Commerce Rules in the context of digital commerce: a mixed-methods study combining statutory analysis with a 290-respondent survey on trust formation in Indian e-commerce (Chawla & Kumar, 2022); a comprehensive provision-by-provision doctrinal analysis of the 2019 Act, the E-Commerce Rules, and related case law (Aher & Sable, 2021); a historical-comparative account of the deficiencies of the 1986 Act and the drafting rationale for the 2019 Act (Patra, 2021); and a recent doctrinal evaluation focused specifically on the CCPA's regulatory performance and residual enforcement gaps (Tamilmani & Archana, 2025). Rather than summarising each source sequentially, the review organises findings thematically around cross-border trade, data protection, and digital governance, in order to surface points of convergence, tension, and omission across the literature.

IV. Literature Review

A. The Scale and Cross-Border Character of E-Commerce Growth

Both Chawla and Kumar (2022) and Aher and Sable (2021) situate their analyses against a backdrop of rapid, internationally entangled growth. Chawla and Kumar note that global cross-border B2C e-commerce was estimated to cross US$1 trillion by 2020, with the number of cross-border shoppers rising from 361 million in 2015 to a projected 994 million by mid-2020. Asia-Pacific alone accounted for over 70% of global e-commerce activity, and India's e-commerce industry grew from roughly US$12.1 billion in online spending in 2015 to an estimated US$167.8 billion by 2020, a compound annual growth rate of approximately 23% (Chawla & Kumar, 2022). Aher and Sable (2021) update this trajectory further, reporting that Indian e-commerce sales increased by 7–8% in 2020 despite pandemic disruption, that India's festive sale season in 2020 alone generated Rs 58,000 crore (approximately US$8.3 billion) in gross sales, and that global investment flows, including Facebook's and Google's multi-billion-dollar investments in Reliance Jio Platforms, have deepened the cross-border financial entanglement of the Indian e-commerce sector.

This scale is precisely what generates jurisdictional strain: a marketplace model may host sellers based abroad, source goods internationally, and route payments through intermediaries subject to different regulatory regimes than the consumer's home jurisdiction. Chawla and Kumar (2022) note that the OECD's 1999 and 2016 guidelines on consumer protection in e-commerce were designed primarily with cross-border transactions in mind, underscoring that the jurisdictional problem is not unique to India but a general feature of e-commerce that domestic legislatures must adapt international guidance to address.

B. Jurisdictional Gaps and the Evolution of the Legal Framework

Patra (2021) offers the most detailed account of why the Consumer Protection Act, 1986 proved unworkable for cross-border and online disputes. Under Section 11 of that Act, a complaint could only be filed within the local limits of the jurisdiction where the opposite party resided, carried on business, or personally worked for gain, or where the cause of action wholly or partly arose. This rule assumed a fixed, locatable seller and broke down when applied to online marketplaces whose registered offices were frequently situated far from the consumer, or outside India altogether, giving rise to what Patra terms jurisdiction hunting. Compounding this, online negotiations and electronic records lacked clear recognition as valid contracts or admissible evidence under the Contract Act, the Evidence Act, the Indian Penal Code, the Indian

Stamp Act, and the Information Technology Act, 2000 as they then stood, statutes drafted, in Patra's words, when e-commerce businesses were not prevalent.

The Consumer Protection Act, 2019 addressed the jurisdictional problem directly in two ways. First, Section 34(2)(d) permits complainants to file where they themselves reside or work for gain, rather than only where the opposing party is located (Patra, 2021), a reform Patra characterises as offering meaningful relief to consumers who previously could not afford to litigate at a distant defendant's location. Second, Aher and Sable (2021) note that the Act's definition of e-commerce under Section 2(16) and its coverage of electronic service providers under Section 2(17) extend its territorial reach to cover e-commerce entities offering goods or services to Indian consumers even where the entity is not established in India, consistent with Rule 2(v) of the E-Commerce Rules, 2020.

Nonetheless, neither Patra (2021) nor Aher and Sable (2021) suggest that jurisdictional questions are fully resolved. Aher and Sable observe that the 2019 Act provides no statutory time frame for the disposal of consumer disputes. This means that even where jurisdiction is correctly established over a cross-border respondent, enforcement may proceed without a defined endpoint, a governance gap distinct from, but compounding, the jurisdictional extension itself. Table 1 summarises the principal structural differences between the two regimes as documented in the literature.

Key Factor	Act, 1986	Act, 2019
Regulating authority	No separate regulator	CCPA established to consider disputes and grievances on unfair contracts
E-commerce	No provision	Explicit definition and coverage of e-commerce, electronic service providers, and online marketplaces
Product liability	No provision	Dedicated claim mechanism for product liability (Ss. 82–87)
Alternative dispute redress	No provision	Mediation cells at District, State, and National levels (Ss. 74–81)
Filing jurisdiction	Complaint filed where opposite party resides or works for gain	Complaint may also be filed where the complainant resides or works for gain
Pecuniary jurisdiction (District)	Up to Rs 1 million	Up to Rs 10 million (later revised upward)

Table 1: Comparison of Key Provisions: Consumer Protection Act, 1986 vs. 2019

C. Product Liability as a Cross-Border Accountability Mechanism

A feature of the 2019 Act with direct relevance to cross-border trade is its product liability regime, introduced for the first time and detailed extensively by Aher and Sable (2021). Section

82 permits a complainant to claim compensation for harm caused by a defective product, and Sections 84 through 87 allocate liability separately across product manufacturers, product service providers, and product sellers. Notably, Section 86 provides that a product seller who is not the manufacturer may still be held liable where the identity of the manufacturer is unknown, or where, if known, the service of notice or process cannot be effected on him because he is not subject to Indian law, a provision squarely aimed at the cross-border scenario in which the ultimate manufacturer is beyond the practical reach of Indian process. This shifts accountability toward the domestic seller or marketplace precisely in cases where the source of the defect is a foreign entity outside the jurisdiction's practical enforcement reach, functioning as a partial substitute for the enforcement gap identified above.

D. Data Protection Within the Consumer Protection Framework

Data protection surfaces across the literature as a significant but only partially addressed concern. Chawla and Kumar (2022) describe data protection as arguably the most severe risk of e-commerce, noting that marketplaces witness frequent violations and that compliance with data-protection regimes such as the European Union's General Data Protection Regulation imposes a considerable expense on e-commerce firms seeking to preserve consumer data safely across jurisdictions. Their survey of 290 Indian online consumers found that privacy of shared personal information was a statistically significant predictor of consumer trust ($p = 0.011$), with a mean importance rating of 4.92 out of 5 among monthly and twice-monthly online shoppers, comparable in magnitude to security ($p = 0.002$) and warranty considerations ($p = 0.027$) as predictors of trust. Notably, trust in privacy protection dropped sharply among the heaviest-frequency shoppers in one reported cell, a divergence the original study does not explain but which may merit further empirical attention.

Within the statutory text itself, the Consumer Protection Act, 2019 addresses data protection indirectly rather than as a freestanding regulatory subject. Section 2(47)(ix), as detailed by Aher and Sable (2021), classifies the disclosure of a consumer's confidential personal information by an electronic service provider, without consent, as an unfair trade practice. This gives consumers a remedy under consumer law even though the Act is not a dedicated data protection statute. The Consumer Protection (E-Commerce) Rules, 2020 supplement this indirectly: Rule 5(3) requires marketplace e-commerce entities to disclose information on available payment methods and the protection of such forms of payment, and Rule 4(9) prohibits e-commerce entities from recording consumer consent automatically, including in the form of pre-ticked checkboxes, a provision that, while framed around consent rather than data protection *per se*, functions as an early regulatory response to what would now be recognised as a manipulative design pattern in digital interfaces.

Tamilmani and Archana (2025) extend this observation into the present, listing data privacy concerns alongside misleading advertisements and counterfeit goods as persistent risks that the 2019 framework has not fully neutralised, and noting that concerns related to data privacy, misleading advertisements, and the absence of effective grievance redressal mechanisms have intensified the need for stronger legal protection for consumers engaged in online transactions. Notably, none of the four sources examines in depth how India's dedicated data protection legislation interacts with, reinforces, or potentially conflicts with the consumer protection regime, nor do any of the sources address cross-border data transfer restrictions as a distinct compliance obligation for e-commerce entities, a gap this review returns to below.

E. Institutional Architecture: The CCPA and the Marketplace/Inventory Distinction

A central institutional innovation across the reviewed literature is the Central Consumer Protection Authority, established under Sections 10 and 18 of the 2019 Act. Aher and Sable (2021) detail its powers comprehensively: *suo motu* investigation of consumer rights violations and unfair trade practices, initiation of inquiries and lawsuits, orders for the recall of dangerous or unsafe goods and services, suspension of unethical commercial practices and false advertisements, and the imposition of penalties on suppliers, endorsers, or publishers of false advertising. Under Section 21, penalties for harmful or repeatedly false advertisements can reach a fine of Rs 5 million with imprisonment of up to five years on a manufacturer or endorser for subsequent offences, alongside bans of up to three years for repeated violations.

The Consumer Protection (E-Commerce) Rules, 2020 operationalise CCPA oversight at the platform level by distinguishing marketplace e-commerce entities, which provide an information-technology platform facilitating transactions between independent buyers and sellers, from inventory e-commerce entities, which own and directly sell their own inventory (Aher & Sable, 2021). Marketplace entities under Rule 5 must ensure sellers accurately describe goods, disclose seller identity and geographic address for effective dispute resolution, and maintain records enabling identification of sellers who have repeatedly offered goods previously removed under copyright, trademark, or information technology law. Sellers themselves, under Rule 6, cannot misrepresent themselves as consumers to post reviews, must maintain a prior written contract with the marketplace entity, and must appoint their own grievance officer. Inventory entities, under Rule 7, bear liability for authenticity where they explicitly or implicitly vouch for the genuineness of goods sold. This tri-partite structure (platform, seller, and consumer) is the Rules' central mechanism for allocating responsibility in a disintermediated, potentially cross-border transaction chain.

Tamilmani and Archana's (2025) more recent assessment finds that the CCPA has genuinely improved regulatory oversight and accountability, particularly through disclosure mandates on seller information, pricing, and return policies, and that the introduction of product liability provisions has increased the accountability of manufacturers, sellers, and service providers for defective products or deficient services sold through online platforms. Yet their analysis also identifies the limits of this architecture: in marketplace models involving numerous third-party sellers, liability of e-commerce intermediaries remains ambiguous, and monitoring of cross-border e-commerce transactions is explicitly listed among the unresolved enforcement challenges. This finding echoes Chawla and Kumar's (2022) earlier caution that the Act and Rules, being new at the time of their study, required at least two years of operational experience before their effectiveness could be fairly assessed, a caution that appears only partly resolved five years later, based on Tamilmani and Archana's continued identification of the same structural ambiguities.

F. Mediation and Alternative Dispute Resolution

Both Aher and Sable (2021) and Patra (2021) highlight the 2019 Act's introduction of statutory mediation as a governance tool relevant to cross-border and platform disputes, where formal litigation against a distant or foreign respondent may be impractical. Sections 74 through 81 establish mediation cells operating at the district, state, and national commission levels, and Section 81(1) provides that no appeal lies against an order passed through mediation, which Aher and Sable suggest is intended to make the redress process at the initial stage speedy for both consumers and service providers. Patra (2021) similarly frames mediation as enabling parties to settle disputes by amicable means in a quicker way, though he notes this route is available only where both parties consent to refer the dispute to mediation, a limitation that may reduce its utility precisely in adversarial cross-border disputes where a foreign respondent has little incentive to participate voluntarily.

G. Consumer Trust and the Limits of Legal Awareness

A recurring, almost paradoxical finding across the literature is that legal reform has outpaced consumer awareness of that reform. Chawla and Kumar (2022), applying Mayer et al.'s (1995) Ability-Benevolence-Integrity model of trust, found that while security, privacy, warranty, customer-service, and website-information factors together strongly predicted consumer trust (overall R-squared = 0.82, p = 0.032), direct awareness of the 2019 Act and 2020 Rules scored markedly lower among survey respondents, with mean values of only 3.14 to 3.42 out of 5, compared to mean values above 4.8 for security and privacy factors. This suggests that consumers value the protections these laws are meant to deliver far more than they are aware the laws themselves exist. Tamilmani and Archana (2025) reach a materially identical conclusion three years later, reporting that despite these legal provisions, consumer awareness regarding rights and legal remedies in e-commerce transactions remains relatively low, which limits the effective utilisation of consumer protection mechanisms. The persistence of this finding across a multi-year gap between studies suggests that the awareness gap is not a transitional artefact of a newly enacted law but a structural feature of the regime as currently implemented.

V. Discussion: Synthesising Emerging Issues

Read together, the four studies point to three emerging issues that existing frameworks address only partially, each of which is elaborated below.

A. Cross-Border Enforcement Lags Behind Jurisdictional Reach

The 2019 Act extends jurisdiction to foreign-based e-commerce entities serving Indian consumers (Aher & Sable, 2021) and allows consumers to file where they reside rather than where the respondent is located (Patra, 2021). Yet no source identifies a corresponding enforcement mechanism capable of compelling compliance from an entity with no assets, bank accounts, or legal presence in India. The product liability provisions of Section 86 partially compensate for this by shifting liability toward a domestically reachable seller when the foreign manufacturer cannot be served process (Aher & Sable, 2021), but this is a workaround for individual product-defect claims rather than a general solution to cross-border enforcement of consumer judgments, refund orders, or CCPA directives. This represents a genuine governance asymmetry: jurisdiction has been extended further than enforceability, and the absence of statutory dispute-resolution timelines (Aher & Sable, 2021) compounds the problem by leaving even domestically enforceable claims without a defined resolution horizon.

B. Data Protection Remains a Derivative, Not a Freestanding, Regulatory Domain

Data protection is currently absorbed into consumer protection law as an instance of unfair trade practice under Section 2(47)(ix), triggered only upon unauthorised disclosure of information already collected, rather than treated as a freestanding regulatory domain governing the fuller life cycle of data collection, processing, cross-border transfer, and breach notification that modern e-commerce entails. Chawla and Kumar's (2022) trust data suggests consumers care about this issue substantially, rating privacy protections nearly on par with core security, yet the statutory hook available to redress a privacy harm remains narrow. Neither Aher and Sable (2021) nor Tamilmani and Archana (2025) identify any provision in the 2019 Act or its Rules that specifically addresses cross-border data transfer, data localisation, or breach notification, obligations increasingly central to comparable international frameworks. This narrow statutory scope stands in some tension with the weight consumers themselves place on data privacy as a determinant of trust.

C. Digital Governance Institutions Face Unresolved Platform-Liability Ambiguity

Digital governance institutions such as the CCPA have expanded regulatory capacity on paper but face practical limits in multi-seller marketplace environments and cross-border scenarios, a limitation acknowledged explicitly in the most recent literature (Tamilmani & Archana, 2025). The marketplace/inventory distinction in the E-Commerce Rules (Aher & Sable, 2021) provides a formal allocation of duties, but formal allocation does not resolve the practical difficulty of identifying which of many third-party sellers on a single platform is responsible for a given harm, particularly where that seller may itself be based outside India. Combined with the absence of statutory timelines for dispute resolution and persistently low consumer awareness (Chawla & Kumar, 2022; Tamilmani & Archana, 2025), this suggests that institutional design alone cannot resolve enforcement gaps without complementary investment in consumer education, platform-level monitoring capacity, and possibly international regulatory cooperation of the kind envisaged, at a broader level, by OECD and UNCTAD guidelines on cross-border consumer protection (Chawla & Kumar, 2022).

VI. Gaps in the Existing Literature

Several gaps are apparent in the reviewed body of work. First, none of the four studies examines the interaction between India's consumer protection regime and its dedicated data protection legislation in operational detail, leaving open how the two regimes might jointly govern a cross-border data breach affecting e-commerce consumers. Second, no source offers empirical data specifically on cross-border enforcement outcomes, that is, how many cross-border disputes filed under the extended jurisdictional provisions of Section 34(2)(d) have actually resulted in enforceable remedies against foreign respondents. Third, while Rule 4(9)'s prohibition on automatically recorded consent (via pre-ticked checkboxes) and Rule 4(7)'s prohibition on unjustified price manipulation gesture toward what contemporary literature elsewhere terms dark patterns in digital interface design, none of the four sources engages with this emerging regulatory concern by name or examines its enforcement record. Fourth, the empirical study by Chawla and Kumar (2022), though methodologically the most rigorous of the four, relies on

 [ISSN 2581-5369]

convenience sampling from a single data-collection window shortly after the Rules came into force, meaning its trust and awareness findings may not reflect the framework's current operational maturity, a limitation only partly addressed by the more recent, though purely doctrinal, work of Tamilmani and Archana (2025). Future research combining updated empirical trust surveys with cross-border enforcement case tracking would substantially strengthen the evidentiary basis for policy reform.

VII. Recommendations

Based on the synthesised literature, this review suggests five directions for reform. First, regulatory authorities should pursue bilateral or multilateral cooperation mechanisms, analogous to the OECD- and UNCTAD-endorsed international consumer-protection networks referenced by Chawla and Kumar (2022), to make cross-border enforcement of consumer judgments and CCPA directives practicable rather than merely jurisdictionally possible. Second, consumer protection rules should be more explicitly harmonised with data protection law, particularly regarding cross-border data transfers, data retention, and breach notification obligations inherent in international e-commerce, moving beyond the current narrow unfair-trade-practice hook. Third, marketplace liability rules should be clarified further, potentially through amendment to Rule 5, to reduce the ambiguity that arises when multiple third-party sellers operate through a single platform (Tamilmani & Archana, 2025). Fourth, the Act should be amended to introduce statutory timelines for the disposal of consumer disputes, addressing the gap identified by Aher and Sable (2021) and reducing the risk that cross-border cases proceed indefinitely. Fifth, sustained public consumer-education campaigns are needed to close the awareness gap that both Chawla and Kumar (2022) and Tamilmani and Archana (2025) identify, three years apart, as a persistent constraint on the practical effectiveness of an otherwise comprehensive legal framework.

VIII. Conclusion

The literature reviewed here shows that India's consumer protection framework has evolved substantially to meet the challenges of e-commerce, replacing a jurisdictionally rigid 1986 statute with a more flexible, institutionally robust 2019 Act, a dedicated E-Commerce Rules regime, and a purpose-built regulatory authority in the CCPA. Provisions on product liability, marketplace and seller duties, and statutory mediation each represent genuine responses to the specific governance challenges that online, cross-border, multi-seller commerce presents. Yet emerging issues in cross-border trade, data protection, and digital governance persist precisely because legal comprehensiveness has not been matched by enforcement capacity, data-

 [ISSN 2581-5369]

protection integration, or consumer awareness. Jurisdiction has been extended further than judgments can practically be enforced; data protection remains a derivative concern within trade-practice law rather than a freestanding regulatory domain; and platform liability, though formally allocated, remains ambiguous in practice. As cross-border e-commerce continues to expand and data-intensive, platform-mediated business models proliferate, the next phase of reform will likely need to move beyond statutory drafting toward enforcement infrastructure, international regulatory cooperation, clearer platform-liability rules, and sustained consumer education, the very areas in which the reviewed literature, read cumulatively across a five-year span, finds the least measurable progress.

IX. References

Aher, S., & Sable, S. (2021). Regulation of e-commerce in India under Consumer Protection Act, 2019: An overview. *International Journal of Law Management & Humanities, 4*(6), 1547–1559. https://doij.org/10.10000/IJLMH.112425

Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: The emerging trend. *Journal of Business Ethics, 180*(2), 581–604. https://doi.org/10.1007/s10551-021-04884-3

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734.

Patra, C. (2021). Relevance of Consumer Protection Act, 2019 in e-commerce. *Indian Journal of Law and Justice, 12*(1), 291–302.

Tamilmani, S., & Archana, S. (2025). Legal protection for consumers in e-commerce transactions: A study under the Consumer Protection Act, 2019. *International Scientific Journal of Engineering and Management, 4*(10). https://doi.org/10.55041/ISJEM05064

*****