INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

E-COMMERCE AND LAW IN INDIA: A CASE STUDY ON CONSUMER PROTECTION, DATA PRIVACY, AND PLATFORM LIABILITY

AUTHORED BY - MRS. VEENA KUMARI
Teaches at Law Centre 2
Faculty of Law, Delhi University

Abstract

The digital marketplace in India has expanded rapidly in the last decade. E-commerce platforms now shape consumer behaviour, enable new business models, and present complex regulatory and adjudicatory challenges. This paper examines three interlinked legal domains—consumer protection, data privacy, and intermediary/platform liability—as they apply to e-commerce in India. It maps the current statutory architecture (with emphasis on the Consumer Protection Act, 2019 and its E-commerce Rules, the Information Technology Act and Intermediary Rules, and the Digital Personal Data Protection Act, 2023), analyses landmark judicial pronouncements and regulatory instruments, assesses friction points faced by consumers and platforms, and offers targeted recommendations for law, policy and practice.

Keywords:
E-commerce law in India; Consumer Protection Act, 2019; E-commerce Rules, 2020; Digital Personal Data Protection Act, 2023; Intermediary liability; Platform regulation; Data privacy and consent; Online consumer rights; Algorithmic transparency; Safe harbour under IT Act; Digital marketplaces; Regulatory governance in India.

1. Introduction and Methodology

The rapid expansion of e-commerce in India has fundamentally transformed the nature of trade, consumption, and market regulation. Digital platforms now function not merely as facilitators of transactions but as powerful market actors that shape consumer choices, influence pricing

structures, and control access to goods and services. While e-commerce has enhanced efficiency, choice, and accessibility, it has simultaneously generated complex legal and regulatory concerns. Issues such as misleading advertisements, unfair trade practices, opaque pricing mechanisms, misuse of consumer data, and the ambiguous legal responsibility of platforms for third-party sellers and content have increasingly come before courts and regulators. In this context, the traditional legal frameworks governing contracts, consumer protection, and liability have required significant adaptation to respond effectively to the realities of digital marketplaces. This paper proceeds from the premise that law must evolve alongside technology, while remaining anchored in principles of fairness, accountability, and consumer welfare.

Against this backdrop, the primary objective of this study is to critically examine the evolving legal framework governing e-commerce in India, with particular focus on consumer protection, data privacy, and platform liability. By analysing key statutory instruments such as the Consumer Protection Act, 2019, the Consumer Protection (E-commerce) Rules, 2020, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, the paper seeks to identify both the strengths and limitations of the existing regulatory regime. Judicial interpretations, especially by the Supreme Court of India, are examined to understand how courts have navigated the balance between safeguarding consumer rights and preserving intermediary autonomy and innovation. The study aims not only to highlight doctrinal developments but also to assess their practical implications for consumers, platforms, and regulators in India's rapidly expanding digital economy.

Methodologically, the author relies primarily on authoritative sources, including statutes, subordinate legislation, reported judicial decisions, and official policy documents. These are supplemented by selected academic literature and policy analyses to provide contextual depth and comparative insight. The analysis follows standard legal-scholarly practices of identifying legal issues, interpreting statutory provisions, examining judicial reasoning, and evaluating regulatory outcomes. Through this methodology, the paper seeks to develop balanced and normative recommendations that are legally sound, practically feasible, and sensitive to the broader constitutional and socio-economic context within which e-commerce regulation in India operates.

2. Legal framework: statutes, rules and judicial contours

This section outlines the principal laws and rules governing consumer protection, data privacy, and intermediary liability as applicable to e-commerce in India.

2.1 Consumer protection: Act and e-commerce rules

The Consumer Protection Act, 2019 (CPA 2019) modernised India's consumer law architecture, introducing provisions that reflect digital commerce realities—alternate dispute resolution mechanisms, stricter obligations on unfair trade practices, and a statutory nod to e-commerce platforms' responsibilities (including provisions empowering the Central Consumer Protection Authority). Building on the CPA, the Consumer Protection (E-commerce) Rules, 2020 set out sector-specific duties for e-commerce entities: obligations to disclose marketplace and seller information, mechanisms for grievance redressal, mandatory cancellation/refund processes, and special prohibitions against manipulative practices such as pseudo-discounting and biased search ranking. These rules attempt to place the onus of transparency and prompt redress on platforms while preserving market dynamism.

2.2 Data protection and privacy

Until 2023, India lacked a dedicated omnibus data-protection statute; data governance relied on sectoral rules and constitutional principles. The Digital Personal Data Protection Act, 2023 (DPDP Act 2023) represents the first comprehensive legislative framework to govern collection, processing, storage, retention and cross-border transfer of digital personal data, while recognising legitimate business processing needs and national security exceptions. The statute introduces duties for data fiduciaries (broadly, platforms) including lawful processing bases, purpose limitation, notice and consent obligations, and individual rights (access, correction, grievance redress). Since enactment, rules and operational guidance have been developed to operationalise compliance expectations for platforms and service providers. Because e-commerce relies heavily on profiling and targeted marketing, the DPDP Act substantially affects how platforms design recommendation systems, targeted advertising and data retention policies.

2.3 Intermediary (platform) liability: IT Act and Rules

Intermediaries—defined broadly to include hosting providers, social media platforms, and marketplace operators—occupy a special place in Indian law. Section 79 of the Information Technology Act, 2000 (IT Act) historically granted a "safe harbour" to intermediaries for third-party content so long as certain due diligence and takedown duties were observed. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 updated intermediary governance by imposing layers of compliance: appointment of grievance officers and nodal contacts, timelines for removal on receiving grievances, and record retention duties. The combination of Section 79 and the 2021 Rules recalibrates intermediary responsibility—safe harbour is conditional on rule compliance. Judicial interpretation has been central to defining the contours of liability and state power under the IT Act.

2.4 Judicial landmarks shaping the field

Two categories of cases have had out-sized influence:

1. **Constitutional and intermediary law** — *Shreya Singhal v. Union of India* (2015) is foundational for online speech and intermediary liability. The Supreme Court struck down Section 66A of the IT Act as unconstitutional and clarified that intermediaries' liability under Section 79 must be read narrowly—intermediaries lose safe harbour only upon court/authority orders or clear "actual knowledge" in a restricted sense. This ruling protected intermediaries and speech but left unresolved tensions when other statutes or executive orders require takedowns.
2. **Intermediary liability in practice** — *Google India Pvt. Ltd. v. M/s Visakha Industries & Anr.* (2019) and subsequent decisions examined whether intermediaries can be treated as publishers or be held liable for user content, including in defamation contexts. The Supreme Court's approach in this and related cases shows that intermediaries may, in particular situations, be subject to criminal liability when they fail to meet statutory duties or where they exhibit knowledge and control over content. These judicial developments indicate that safe harbour is not absolute and that fact-sensitive inquiries will determine liability.

3. Core issues and case studies

This section analyzes key friction points that arise when consumer protection, privacy, and intermediary liability intersect in the e-commerce ecosystem. Each issue is illustrated with statutory context and judicial or regulatory examples.

3.1 Transparency, mis-representation and unfair trade practices

E-commerce platforms host millions of listings and third-party sellers who may misrepresent product quality, delivery timelines or pricing. The CPA 2019 and the 2020 E-commerce Rules mandate disclosure duties (seller identity, return/refund terms), but enforcement remains uneven. Consumers often report "drip pricing" (hidden charges added at checkout), misleading "original price" versus "discounted" price tactics, and difficulty obtaining timely refunds (despite rules requiring prompt refund mechanisms). The law provides tools—consumer fora, the Central Consumer Protection Authority (CCPA) and penal provisions—but the scale of online transactions strains resources and reveals a need for proactive platform compliance and algorithmic transparency rather than reactive adjudication.

3.2 Algorithmic bias, search ranking and platform conduct

Platforms exercise editorial control through algorithms—curation, ranking, recommendations and "sponsored" placements. The E-commerce Rules proscribe manipulative practices that disadvantage consumers or small sellers (for example, biased search results that give undue prominence to a platform's inventory or preferred sellers). Yet the opacity of proprietary ranking algorithms impedes meaningful scrutiny. Consumers and regulators thus face an information asymmetry: platforms know their ranking rules and promotional logics; consumers do not. The DPDP Act's obligations (especially purpose limitation and transparency requirements) nudge platforms to disclose more about profiling practices when they materially influence consumer choice—but precise regulatory standards for algorithmic audits, non discrimination and access to explanations are still maturing internationally and domestically. This legal uncertainty harms consumer trust and can entrench dominant players' market power if left unaddressed.

3.3 Data collection, targeted advertising and consent fatigue

E-commerce platforms collect a wide array of personal and behavioural data: purchase history, browsing patterns, payment information, geolocation, and device identifiers. Targeted advertising and personalization provide consumer value but also increase privacy risk. The DPDP Act institutes lawful bases for processing and individual rights; however, in practice, consent mechanisms are often granular but opaque, and "consent fatigue" results when users click through dense policies. Platforms tend to default towards extensive profiling because of its commercial value, potentially at the cost of user autonomy. The law requires meaningful notice and opt-out paths, and data fiduciaries must implement data minimisation and purpose limitation. Effective enforcement—audits, penalties and accessible redress—will determine if the statutory promises translate into user control.

3.4 Intermediary safe harbour: practical frictions and criminal defamation

The theoretical safe harbour in Section 79 has been constricted through judicial interpretation and subsequent rules. *Shreya Singhal* protected intermediaries from arbitrary takedowns but the 2021 Rules and court decisions have required intermediaries to maintain grievance redress systems, appoint compliance officers, and react to government orders. The *Google India v. Visakha* litigation demonstrated that intermediaries can be pulled into criminal proceedings as accused publishers under certain conditions. The practical problem for platforms: balancing fast, automated content moderation (necessary at scale) with due process and accuracy to avoid wrongful takedowns and legal liability. For consumers, prompt takedowns can be crucial to preventing harm; for platforms, knee-jerk takedowns may chill lawful speech and commerce. The law's step-incentives (penalties for non-compliance vs. protections for good faith moderation) thus need careful calibration.

3.5 Cross-border data flows, jurisdiction and enforcement

Many e-commerce platforms operate across borders, and user data may be processed in multiple jurisdictions. The DPDP Act and complementary rules address cross-border transfer regimes and impose conditions to protect Indian users' personal data. However, enforcement against foreign entities raises jurisdictional challenges; mutual legal assistance and international cooperation become important. Additionally, small sellers and consumers using global platforms may lack

local remedies, requiring innovative mechanisms such as designated local grievance officers and stronger platform obligations to maintain enforceable remedies within India.

4. Analysis: tensions, lacunae and normative choices

This section synthesizes the preceding analysis and identifies principled tensions as well as legal gaps that deserve attention.

4.1 Regulating conduct vs. regulating code

One fundamental policy question is whether law should regulate platform conduct (terms, marketplace policies, disclosure, warranties) or the code/algorithms that produce outcomes (ranking systems, recommendation engines). Conduct rules—like those in the CPA and E-commerce Rules—are easier to draft and enforce; they require platforms to disclose, to process refunds, and to maintain redress systems. Code regulation (algorithmic audits, source-level transparency) is technically difficult and raises proprietary-rights concerns. Yet, without some regulatory approach to algorithmic accountability, platforms can comply with disclosure norms while maintaining opaque control over outcomes that materially affect consumer choice. A blended approach—mandating outcome audits and disclosed key parameters, without forcing open source—may be the most pragmatic and proportionate route.

4.2 Liability incentives and unintended consequences

Overly broad intermediary liability risks chilling innovation and expression; overly narrow liability risks leaving consumers and small sellers without remedy. Judicial decisions show that Indian courts will not permit absolute immunity when intermediaries clearly control or profit from contested content. The law should therefore calibrate liability to the intermediary's level of control and awareness: passive hosting should retain a degree of protection, while active curation, monetisation and editorial intervention should attract commensurate duties. This "control-and-profit" test aligns incentives: platforms that profit and exercise editorial control must also invest in governance to reduce harms.

4.3 Privacy vs. personalization tradeoffs

Targeted recommendations increase consumer welfare via personalization but depend on data processing. The DPDP Act tries to reconcile this by allowing lawful processing for business purposes while preserving user rights. Practically, a risk-based approach to data processing—where high-risk profiling (e.g., for financial decisions) triggers stricter safeguards and audit requirements—would allow benign personalization while restricting intrusive practices. Default privacy-protective settings and transparent opt-in for high-risk processing would reduce consent fatigue and reinforce user control.

4.4 Procedural safeguards and access to justice

The CPA and E-commerce Rules provide for grievance redressal, but procedural access remains unequal. Many consumers lack awareness of formal fora or the wherewithal to litigate. The state could incentivise alternative dispute resolution (ODR) mechanisms embedded within platforms, overseen by the CCPA for quality control. These ODR systems must be free, speedy and designed to avoid procedural traps (complex forms, opaque evidence rules).

5. Recommendations

Based on the statutory landscape, judicial precedents, and the policy tensions identified, the following recommendations are proposed. They are grouped into legislative/regulatory reforms, platform governance measures, and judicial/practical interventions.

5.1 Legislative and regulatory reforms

1. **Algorithmic accountability statute or rulebook:** Introduce rules under existing statutes requiring platforms to disclose non-proprietary summaries of ranking and recommendation logics, criteria for sponsored content, and audit trails for major changes in ranking logic. Disclosure should be outcome-oriented (e.g., "sponsored listings may appear as top three results when seller pays for placement") rather than forced source-code release.
2. **Risk-based data processing framework:** Implement DPDP Act secondary rules that categorise types of profiling (low, medium, high risk) and attach graduated obligations: stronger consent and audit for high-risk uses such as credit scoring or employment profiling.

3. **Harmonised cross-statutory compliance standards:** Create a single e-commerce compliance charter that harmonises CPA/E-commerce Rules, IT Rules, and DPDP principles—so platforms can implement a unified compliance suite rather than conflicting checklists.
4. **Stronger penalties for deceptive trade practices with swift interim relief:** Empower consumer authorities to grant prompt interim relief (e.g., freezing seller accounts, provisional refunds) in cases of mass deception while investigations proceed.

5.2 Platform governance and market practice

1. **Design for redress:** Platforms should embed ODR mechanisms with easy prelitigation remedies (chatbot-assisted claims, human escalation in 48 hours for high-value disputes). Platforms must publish quarterly dispute resolution metrics.
2. **Privacy by default & data minimisation:** Default settings should limit unnecessary data collection. If personalization requires more data, platforms should seek explicit, granular opt-ins and provide easily usable opt-outs.
3. **Independent algorithmic audits:** Platforms above a turnover threshold should commission independent algorithmic audits annually and make summaries public. Audit focus should be on discriminatory outcomes, hidden promotions and consumer harm.
4. **Seller vetting and reputational guarantees:** For marketplaces, stronger seller verification and insurance/escrow for high-value transactions would protect consumers and reduce fraudulent listings.

5.3 Judicial and enforcement practice

1. **Specialised benches and ADR for digital commerce disputes:** Courts and consumer fora could create fast-track channels for e-commerce disputes, with technical experts on panels where algorithmic or data issues are central.
2. **Guidelines for intermediary takedown:** The judiciary should continue to refine standards for "actual knowledge" and clarify procedures for emergency takedowns that preserve due process—e.g., mandatory notice to the publisher and an expedited review window when possible.

3. **Cooperation with global regulators:** The Indian regulators should engage in bilateral and multilateral frameworks to manage cross-border enforcement, data requests and platform accountability.

6. Conclusion

E-commerce in India sits at a legal crossroads. The modernised Consumer Protection Act, the 2020 E-commerce Rules, the 2021 IT Rules, and the DPDP Act of 2023 together represent a mature statutory toolkit. Judicial decisions such as *Shreya Singhal* and *Google India v. Visakha* demonstrate the courts' role in clarifying contours of liability and free speech in digital environments. Despite this progress, important gaps remain: algorithmic opacity, consent fatigue, cross-border enforcement problems, and unequal access to redress. A combination of targeted legislative tweaks, robust platform governance, independent audits, and judicially crafted procedural safeguards can push India's regulatory ecosystem toward a pragmatic balance—protecting consumers' rights and privacy while allowing platforms to innovate.

For practitioners and scholars, the task now is to translate these legal tools into operational compliance—clearer disclosure regimes, meaningful consent and data minimisation, and well-designed ODR systems. For lawmakers and regulators, the challenge is to craft proportionate rules that focus on outcomes (consumer harm) rather than blunt instrument regulation of code. If India succeeds in this balancing act, it can offer a model for other jurisdictions grappling with the same tensions between commerce, privacy, and platform power.

Bibliography

1. **Consumer Protection Act, 2019.** Government of India. (Statute). (Text: *The Consumer Protection Act, 2019*).
2. **Consumer Protection (E-commerce) Rules, 2020.** Ministry/Official Gazette. (Regulations governing e-commerce platforms).
3. **The Information Technology Act, 2000.** (Statute; especially Section 79 on intermediary immunity).

4. **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.** Ministry of Electronics & Information Technology (MeitY). (Rules clarifying intermediary duties and grievance redressal).
5. **The Digital Personal Data Protection Act, 2023.** Government of India (Parliamentary enactment establishing a statutory framework for digital personal data).
6. **Shreya Singhal & Ors. v. Union of India & Ors.** (Writ Petition (Criminal) No. 167 of 2012), Supreme Court of India, Judgment dated 24 March 2015 (landmark on Section 66A and intermediary liability).
7. **Google India Pvt. Ltd. v. M/s Visakha Industries & Anr.** (Supreme Court of India, 10 December 2019) (case exploring intermediary liability and criminal defamation).