Page 344 - 383 **DOI:** *https://doij.org/10.10000/IJLMH.1111542*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Unfair Trade Practices in India's Digital Economy: A Comparative Analysis of Global Regulatory Approaches

RAJIB KUMAR DAS[1]

ABSTRACT

This article examines the evolving landscape of unfair trade practices in India's digital economy through a comprehensive analysis of consumer protection, competition law, and data privacy frameworks. Using an integrated doctrinal and comparative legal approach, it demonstrates that digital markets present unprecedented challenges to traditional legal frameworks designed for brick-and-mortar commerce. The analysis reveals that unfair trade practices in digital markets are not isolated incidents but systematic patterns arising from structural asymmetries inherent in platform-based ecosystems. Dominant platforms exploit gatekeeper positions, data advantages, and algorithmic capabilities to engage in practices ranging from dark patterns and algorithmic price discrimination to self-preferencing and data exploitation. This article provides a detailed taxonomy of unfair trade practices, analyses the legal framework comprising the Consumer Protection Act, 2019, the Competition Act, 2002, and the Digital Personal Data Protection Act, 2023, and examines enforcement challenges, particularly regarding multinational corporations. Through comparative analysis of regulatory approaches in the European Union, United Kingdom, and United States, the article proposes a multi-pronged regulatory strategy including digital markets-specific legislation, enhanced penalty regimes, strengthened institutional capacity, and cross-border cooperation mechanisms. The research contributes to legal scholarship by providing a comprehensive mapping of the intersection between consumer protection, competition law, and data privacy in India's digital economy, while offering concrete policy recommendations for creating a fair, transparent, and contestable digital marketplace.

Keywords: *Unfair Trade Practices, Digital Economy, Consumer Protection Act 2019, Competition Law, Dark Patterns, Platform Regulation, Algorithmic Manipulation, Data Privacy, E-Commerce Regulation, Digital Markets*

[1] Author is a PhD Research Fellow at Department of Law, University of Burdwan, West Bengal, India.

 [ISSN 2581-5369]

I. INTRODUCTION

A. Research Problem and Context

India's digital economy has experienced exponential growth over the past decade, with e-commerce retail sales projected to reach USD 350 billion by 2030 and digital payments transactions exceeding 100 billion annually.[2] This rapid digitalization has fundamentally transformed commercial relationships, creating new forms of market intermediation through platform-based ecosystems that connect consumers, businesses, and service providers. However, this transformation has also given rise to novel forms of unfair trade practices that exploit the unique characteristics of digital markets information asymmetries, network effects, data advantages, and algorithmic capabilities to the detriment of consumers and smaller market participants.[3]

The structural characteristics of digital markets differ fundamentally from traditional brick-and-mortar commerce. Platform businesses benefit from strong network effects, where the value of the platform increases exponentially with each additional user, creating winner-takes-most dynamics that lead to market concentration.[4] Data-driven externalities enable platforms to leverage user-generated data to improve services, create barriers to entry, and engage in sophisticated forms of price discrimination and behavioural manipulation.[5] Multi-sided market structures allow platforms to subsidize one side of the market while extracting rents from another, obscuring the true economic costs and benefits of platform participation.[6] These characteristics create structural asymmetries that enable dominant platforms to engage in unfair trade practices that are difficult to detect, prove, and remedy under traditional legal frameworks.

Recent enforcement actions by Indian regulators have highlighted the prevalence and sophistication of unfair trade practices in digital markets. The Central Consumer Protection Authority (CCPA) has issued notices to major e-commerce platforms for dark patterns including drip pricing, basket sneaking, and false urgency tactics.[7] The Competition Commission of India (CCI) has initiated investigations into alleged abuse of dominance by major platforms in e-

[2] Ministry of Commerce and Industry, INDIA BRAND EQUITY FOUNDATION REPORT ON E-COMMERCE (2024).
[3] Gupta, Artificial Intelligence and Competition Law in India: A Legal Response to Algorithmic Market Collusions, 15(3) EUR. ECON. LETTERS (2025), https://doi.org/10.52783/eel.v15i3.3450.
[4] Anshuman Sakle et al., The Interaction Between Competition Law & Digital and E-Commerce Markets in India, 16 INDIAN J.L. & TECH. 18 (2022), https://doi.org/10.55496/kvug7838.
[5] Bhat, Data Sharing for Contestability in Data-Driven Digital Markets: An Analysis, 4 CCI J. ON COMPETITION L. & POL'Y 113 (2023), https://doi.org/10.54425/ccijoclp.v4.113.
[6] Jain et al., Regulating Competition in Digital Markets, ICRIER PROSUS CTR. FOR INTERNET & DIGITAL ECON. (2024).
[7] Central Consumer Protection Authority, GUIDELINES FOR PREVENTION AND REGULATION OF DARK PATTERNS, 2023 (2023).

 [ISSN 2581-5369]

commerce, food delivery, and digital payments sectors.[8] The proposed Digital Personal Data Protection Act, 2023, addresses concerns about unfair data collection and processing practices that undermine consumer autonomy and privacy.[9] However, enforcement remains fragmented across multiple regulatory authorities with overlapping jurisdictions, and penalties imposed on multinational corporations have been criticized as insufficient to deter violations.[10]

B. Research Questions and Objectives

This article addresses three central research questions:

First, what constitutes unfair trade practices in India's digital economy, and how do these practices differ from traditional unfair trade practices in brick-and-mortar commerce? This question requires developing a comprehensive taxonomy of digital unfair trade practices that accounts for algorithmic manipulation, interface design deception, data exploitation, and platform-to-business unfair practices.

Second, how effective is India's current legal framework comprising the Consumer Protection Act, 2019, the Competition Act, 2002, and the Digital Personal Data Protection Act, 2023 in addressing unfair trade practices in digital markets? This question necessitates analysing the substantive provisions, institutional mechanisms, and enforcement track record of these legal instruments, with particular attention to gaps, overlaps, and coordination challenges.

Third, what legal reforms and policy interventions are necessary to create a fair, transparent, and contestable digital marketplace in India? This question requires comparative analysis of regulatory approaches in other major jurisdictions and development of context-appropriate recommendations for India.

The objectives of this article are: (1) to provide a comprehensive conceptual framework for understanding unfair trade practices in digital markets; (2) to analyse India's legal and institutional framework for regulating digital markets; (3) to develop a detailed taxonomy of unfair trade practices prevalent in India's digital economy; (4) to examine enforcement challenges, particularly regarding multinational corporations; (5) to conduct comparative analysis of regulatory approaches in the European Union, United Kingdom, and United States; and (6) to propose concrete legal reforms and policy interventions.

[8] Singh, Amazon's Competition Investigation in India: A Case for Expansion of Investigation and Grant of Interim Relief, INDIAN J.L. & TECH. (2020), https://doi.org/10.55496/pkvm6266.
[9] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[10] Tewari, A Critical Evaluation of India's Proposed Digital Competition Act, 5 CCI J. ON COMPETITION L. & POL'Y 197 (2024), https://doi.org/10.54425/ccijoclp.v5.197.

 [ISSN 2581-5369]

C. Scope and Significance

This article focuses on unfair trade practices in India's digital economy, with particular emphasis on e-commerce, digital platforms, and online services. The analysis encompasses consumer-facing practices (dark patterns, algorithmic pricing, deceptive advertising), platform-to-business practices (self-preferencing, unfair contract terms, data exploitation), and competition law concerns (abuse of dominance, anti-competitive agreements). While the article addresses data privacy issues, it does so primarily through the lens of unfair trade practices rather than providing a comprehensive analysis of all aspects of data protection law.

The significance of this research lies in its comprehensive approach to a problem that has traditionally been analysed through separate disciplinary lenses. Consumer protection scholars have focused on deceptive practices and information asymmetries, competition law scholars on market power and anti-competitive conduct, and data privacy scholars on consent and data processing. This article demonstrates that unfair trade practices in digital markets require an integrated analytical framework that recognizes the convergence of these legal domains.[11] The research contributes to ongoing policy debates in India regarding the need for digital markets-specific legislation, drawing lessons from the European Union's Digital Markets Act and similar initiatives in other jurisdictions.[12]

II. LITERATURE REVIEW: DIGITAL MARKETS, COMPETITION, AND CONSUMER PROTECTION

A. Theoretical Foundations of Digital Market Power

The economic literature on digital markets has identified several structural characteristics that distinguish platform-based ecosystems from traditional markets and create conditions conducive to market concentration and unfair trade practices. Network effects, whereby the value of a platform increases with the number of users, create powerful barriers to entry and winner-takes-most dynamics.[13] Direct network effects occur when users on the same side of the market benefit from additional users (e.g., social networks), while indirect network effects arise in multi-sided markets where users on one side benefit from more users on another side (e.g., e-commerce marketplaces connecting buyers and sellers).[14] These network effects create

[11] Padmavathy Nehru, Digital Economy & Competition Law: A Conundrum, INDIAN J. LEGAL REV. (2022).
[12] Ministry of Corporate Affairs, REPORT OF THE COMMITTEE ON DIGITAL COMPETITION LAW (2024).
[13] *Supra* note 3.
[14] *Id.*

tipping points beyond which a dominant platform becomes difficult to displace, even if competitors offer superior services.[15]

Data advantages constitute another critical source of market power in digital markets. Platforms accumulate vast quantities of user data through continuous interactions, enabling them to improve services, personalize offerings, and predict consumer behaviour with increasing accuracy.[16] This creates data-driven feedback loops where more users generate more data, which enables better services, which attracts more users, further entrenching dominance.[17] The value of data is non-rivalrous (multiple parties can use the same data simultaneously) and exhibits increasing returns to scale (more data enables better insights), creating natural monopoly tendencies in data-intensive markets.[18]

Economies of scale and scope in digital markets differ from traditional industries. Marginal costs of serving additional users are often near zero, while fixed costs of platform development are substantial, creating strong incentives for market concentration.[19] Platforms can leverage their infrastructure across multiple markets (economies of scope), enabling conglomerate expansion and creating ecosystems that lock in users across multiple services.[20] These characteristics have led scholars to characterize dominant digital platforms as "gatekeepers" that control access to markets and can extract rents from both consumers and business users.[21]

Recent scholarship has examined how these structural characteristics enable unfair trade practices. Algorithmic collusion can occur when pricing algorithms learn to coordinate without explicit agreement, raising prices above competitive levels while remaining difficult to detect and prove under traditional competition law frameworks.[22] Self-preferencing allows vertically integrated platforms to favour their own products or services over those of competitors, leveraging their gatekeeper position to distort competition.[23] Data exploitation enables platforms to engage in sophisticated forms of price discrimination, behavioural manipulation, and surveillance capitalism that extract consumer surplus while undermining autonomy and privacy.[24]

[15] *Id.*
[16] *Supra* note 4.
[17] *Id.*
[18] *Id.*
[19] *Supra* note 5.
[20] *Id.*
[21] *Supra* note 11.
[22] *Supra* note 2.
[23] *Supra* note 7.
[24] *Supra* note 4.

 [ISSN 2581-5369]

B. Evolution of Competition Law and Consumer Protection in Digital Contexts

Competition law and consumer protection frameworks were developed primarily for industrial-era markets characterized by physical products, transparent pricing, and identifiable market boundaries. The application of these frameworks to digital markets has revealed significant limitations and prompted calls for reform in multiple jurisdictions.[25]

Traditional competition law focuses on consumer welfare, typically measured through price effects and output restrictions. However, many digital services are offered "free" in exchange for user data, making price-based analysis inadequate.[26] The consumer welfare standard has been criticized for failing to account for non-price harms including privacy violations, reduced innovation, and degradation of service quality.[27] Some scholars advocate for a total welfare standard that considers effects on all market participants, including business users and workers, while others propose multi-dimensional welfare metrics that incorporate privacy, autonomy, and innovation.[28]

The ex-post nature of traditional competition law enforcement has proven problematic in fast-moving digital markets. By the time anti-competitive conduct is investigated, adjudicated, and remedied, market structures may have become entrenched and irreversible.[29] This has led to proposals for ex-ante regulation that imposes obligations on dominant platforms before harm occurs, as exemplified by the European Union's Digital Markets Act.[30] However, ex-ante regulation raises concerns about regulatory capture, innovation disincentives, and the difficulty of identifying appropriate regulatory thresholds.[31]

Consumer protection law has similarly struggled to address digital market practices. Traditional prohibitions on false advertising and deceptive practices were designed for explicit misrepresentations, not the subtle behavioural manipulation enabled by algorithmic systems and interface design.[32] Dark patterns user interface designs that trick or manipulate users into making choices they would not otherwise make exploit cognitive biases and bounded rationality in ways that traditional consumer protection law does not adequately address.[33] The concept of

[25] *Supra* note 10.
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Supra* note 9.
[30] Regulation (EU) 2022/1925 of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act).
[31] *Supra* note 9.
[32] Sharma, Dark Patterns in a Bright World: An Analysis of the Indian Consumer Legal Architecture (2024).
[33] Chugh et al., Unpacking Dark Patterns: Understanding Dark Patterns and Their Implications for Consumer Protection in the Digital Economy (2024).

informed consent, central to consumer protection law, becomes problematic when consent is obtained through lengthy, incomprehensible terms of service or manipulative interface designs.[34]

In India, the evolution from the Monopolies and Restrictive Trade Practices Act, 1969 (MRTP Act) to the Competition Act, 2002 reflected a shift from controlling monopolies to promoting competition and consumer welfare.[35] The Consumer Protection Act, 2019 modernized consumer protection law by explicitly addressing e-commerce, unfair trade practices, and product liability, while establishing the Central Consumer Protection Authority with proactive enforcement powers.[36] However, scholars have noted that these frameworks were not designed specifically for digital markets and require further adaptation.[37]

C. Intersections of Data Privacy, Competition, and Consumer Protection

Recent scholarship has increasingly recognized that data privacy, competition law, and consumer protection are interconnected in digital markets, with practices that violate one domain often implicating others.[38] Data has emerged as a critical parameter of competition, with dominant platforms leveraging data advantages to entrench market power and exclude competitors.[39] Privacy violations can constitute unfair trade practices when they involve deceptive data collection or processing that harms consumer interests.[40] Conversely, anti-competitive conduct can undermine privacy by reducing competitive pressure to offer privacy-protective alternatives.[41]

The debate over whether competition authorities should consider privacy harms has generated significant scholarly attention. Some argue that privacy is a quality dimension of competition and should be considered in merger review and abuse of dominance cases.[42] Others contend that privacy regulation should be left to specialized data protection authorities to avoid mission creep and maintain institutional expertise.[43] The German Bundeskartellamt's Facebook decision, which found that exploitative terms of service regarding data collection constituted

[34] Yadav, Strengthening Consumer Consent in E-Commerce: Legal and Policy Reforms to Address Dark Patterns and AI-Driven Challenges (2024).
[35] Competition Act, 2002, No. 12, Acts of Parliament, 2003 (India).
[36] Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).
[37] Pathak, Legal and Commercial Dynamics of E-Consumer Protection: Navigating Challenges in India's Digital Economy, 6(5) INT'L J. FOR MULTIDISCIPLINARY RSCH. (2024), https://doi.org/10.36948/ijfmr.2024.v06i05.28398.
[38] *Supra* note 10.
[39] *Supra* note 4.
[40] *Supra* note 31.
[41] *Supra* note 4.
[42] *Id.*
[43] *Id.*

 [ISSN 2581-5369]

abuse of dominance, exemplifies the integration of privacy and competition analysis.[44]

In India, the intersection of data protection and competition law has been examined by several scholars and policy reports. The Committee on Digital Competition Law recommended that the proposed digital competition legislation should consider data-related practices as potential competition concerns.[45] The Digital Personal Data Protection Act, 2023 includes provisions on data portability that could reduce switching costs and promote competition, though implementation details remain to be specified.[46] Scholars have called for coordinated enforcement between the Data Protection Board, Competition Commission of India, and Central Consumer Protection Authority to address practices that implicate multiple legal domains.[47]

D. Gaps in Existing Literature and Contribution of this Study

While the literature on digital markets regulation has grown substantially, several gaps remain. First, much of the scholarship focuses on global platforms and regulatory approaches in the European Union and United States, with limited attention to the specific context of emerging digital economies like India.[48] Second, existing studies tend to analyse consumer protection, competition law, and data privacy separately, rather than examining their intersections and interactions in addressing unfair trade practices.[49] Third, there is limited empirical research on the prevalence and impact of specific unfair trade practices in Indian digital markets, with most analysis relying on case studies and anecdotal evidence.[50] Fourth, enforcement challenges, particularly regarding multinational corporations with complex corporate structures and cross-border operations, have received insufficient scholarly attention.[51]

This article addresses these gaps by: (1) providing a comprehensive analysis of unfair trade practices specifically in the Indian digital economy context; (2) adopting an integrated analytical framework that examines the convergence of consumer protection, competition law, and data privacy; (3) developing a detailed taxonomy of unfair trade practices based on analysis available literature (4) examining enforcement challenges with particular focus on the multinational corporation accountability gap; and (5) proposing context-appropriate policy recommendations informed by comparative analysis of global regulatory approaches.

---

[44] Bundeskartellamt, FACEBOOK CASE DECISION (2019).
[45] *Supra* note 11.
[46] *Supra* note 8.
[47] *Supra* note 10.
[48] Larionova et al., India. Developing Regulation of Technological Platforms for Digital Economy Growth (2024).
[49] *Supra* note 10.
[50] Tamilmani et al., Impact of Dark Patterns in E-Commerce on Consumer Rights (2024).
[51] *Supra* note 7.

 [ISSN 2581-5369]

III. Legal framework analysis: India's regulatory architecture for digital markets

A. Consumer Protection Act, 2019: Modernizing Consumer Rights

The Consumer Protection Act, 2019 (CPA 2019) represents a significant modernization of India's consumer protection framework, explicitly addressing e-commerce and digital markets for the first time.[52] The Act defines "unfair trade practice" broadly to include any practice that deceives consumers or is likely to deceive them regarding the quality, quantity, potency, purity, standard, or price of goods or services.[53] This definition encompasses false or misleading representations, misleading advertisements, and practices that create confusion about the source, sponsorship, or approval of goods or services.[54]

Section 2(7) of the CPA 2019 defines "consumer" to include any person who buys goods or avails services through electronic means or by teleshopping, explicitly bringing e-commerce transactions within the Act's scope.[55] Section 2(16) defines "e-commerce" as "buying or selling of goods or services including digital products over digital or electronic network," providing a technology-neutral definition that can adapt to evolving business models.[56] Section 2(47) defines "unfair contract" as a contract between a manufacturer or trader or service provider on one hand, and a consumer on the other, having such terms which cause a significant change in the rights of the consumer, including terms that are so adverse to the consumer that they would be inequitable.[57]

The Consumer Protection (E-Commerce) Rules, 2020, issued under Section 101 of the CPA 2019, provide detailed regulations for e-commerce entities.[58] Rule 4 imposes disclosure obligations requiring e-commerce entities to provide information about sellers, total price of goods or services, terms of exchange and return, delivery and shipment, available payment methods, grievance redressal mechanisms, and country of origin.[59] Rule 5 prohibits e-commerce entities from manipulating search results to promote certain sellers, discriminating between sellers of similar goods or services, or adopting any unfair trade practice.[60] Rule 6 addresses mis-selling, requiring e-commerce entities to ensure that advertisements are consistent with

[52] *Supra* note 35.
[53] *Id.* § 2(47).
[54] *Id.*
[55] *Id.* § 2(7).
[56] *Id.* § 2(16).
[57] *Id.* § 2(47).
[58] Consumer Protection (E-Commerce) Rules, 2020 (India).
[59] *Id.* r. 4.
[60] *Id.* r. 5.

actual characteristics of goods or services and that descriptions, images, and other content are accurate.[61]

The establishment of the Central Consumer Protection Authority (CCPA) under Section 10 of the CPA 2019 marked a shift from purely reactive consumer protection to proactive regulation.[62] The CCPA has powers to inquire into violations of consumer rights, investigate, and launch prosecution, issue safety notices and alerts, order recall of unsafe goods or withdrawal of services, and impose penalties.[63] In 2023, the CCPA issued Guidelines for Prevention and Regulation of Dark Patterns, defining dark patterns as "any practices or deceptive design patterns using UI/UX interactions on any platform that is designed to mislead or trick users to do something they originally did not intend or want to do, by subverting or impairing the consumer autonomy, decision making or choice."[64]

The CCPA Guidelines identify thirteen categories of dark patterns: false urgency, basket sneaking, confirm shaming, forced action, subscription trap, interface interference, bait and switch, drip pricing, disguised advertisement, nagging, trick question, SaaS billing, and rogue malware.[65] The Guidelines prohibit platforms from using these practices and require transparency in pricing, clear disclosure of terms and conditions, and respect for consumer choice.[66] Violations can result in penalties under Section 21 of the CPA 2019, including fines up to Rs. 10 lakh for manufacturers or endorsers and up to Rs. 50 lakh for subsequent violations.[67]

However, scholars have identified several limitations in the CPA 2019 framework. First, the penalty provisions are modest compared to the revenues of major digital platforms, potentially making violations a cost of doing business rather than an effective deterrent.[68] Second, the Act does not specifically address algorithmic manipulation, personalized pricing, or other sophisticated forms of digital unfair trade practices.[69] Third, enforcement capacity remains limited, with the CCPA having issued notices to major platforms but securing few final adjudications with substantial penalties.[70] Fourth, the Act's jurisdictional provisions regarding foreign e-commerce entities remain ambiguous, creating challenges for cross-border

[61] *Id.* r. 6.
[62] *Supra* note 35, § 10.
[63] *Id.* § 18.
[64] *Supra* note 6.
[65] *Id.*
[66] *Id.*
[67] *Supra* note 35, § 21.
[68] *Supra* note 36.
[69] *Supra* note 31.
[70] *Supra* note 49.

 [ISSN 2581-5369]

enforcement.[71]

B. Competition Act, 2002: Addressing Market Power Anti-competitive Conduct

The Competition Act, 2002 provides the framework for addressing anti-competitive agreements, abuse of dominance, and combinations (mergers and acquisitions) that may have appreciable adverse effects on competition.[72] Section 3 prohibits anti-competitive agreements, including horizontal agreements (cartels) and vertical agreements that cause or are likely to cause an appreciable adverse effect on competition.[73] Section 4 prohibits abuse of dominant position, defining dominance as a position of strength enjoyed by an enterprise in the relevant market that enables it to operate independently of competitive forces or affect its competitors or consumers or the relevant market in its favour.[74]

Section 4(2) provides a non-exhaustive list of abusive practices including: (a) directly or indirectly imposing unfair or discriminatory conditions or prices in purchase or sale of goods or services; (b) limiting or restricting production, supply, or technical or scientific development; (c) denying market access; (d) making conclusion of contracts subject to acceptance of supplementary obligations; and (e) using dominant position in one market to enter into or protect another market.[75] Section 19(4) specifies factors for determining dominance, including market share, size and resources of the enterprise, size and importance of competitors, economic power including commercial advantages over competitors, vertical integration, dependence of consumers, monopoly or dominant position by statute, entry barriers, countervailing buying power, and market structure and size.[76]

The Competition Commission of India (CCI) has increasingly applied the Competition Act to digital markets, though with mixed results. In the Amazon-Flipkart investigation, the CCI examined allegations that these e-commerce platforms engaged in exclusive agreements with sellers, preferential listing, deep discounting, and other practices that violated Sections 3 and 4 of the Act.[77] In the Google Android case, the CCI found that Google abused its dominant position in the market for licensable smart mobile operating systems by imposing anti-competitive conditions on device manufacturers.[78] In the Meta-WhatsApp privacy policy case,

[71] Ayilyath, Consumer Protection in E-Commerce Transactions in India — Need for Reforms, SSRN (2020), https://doi.org/10.2139/SSRN.3571069.
[72] *Supra* note 34.
[73] *Id.* § 3.
[74] *Id.* § 4.
[75] *Id.* § 4(2).
[76] *Id.* § 19(4).
[77] *Supra* note 7.
[78] Competition Commission of India, GOOGLE ANDROID CASE DECISION (2022) (India).

 [ISSN 2581-5369]

the CCI investigated whether WhatsApp's 2021 privacy policy update constituted abuse of dominance by imposing unfair terms on users.[79]

However, digital markets present several challenges for competition law enforcement. First, defining relevant markets in multi-sided platforms is complex, as traditional market definition methodologies based on substitutability and price effects may not capture platform dynamics.[80] Second, proving abuse of dominance requires demonstrating both dominance and abusive conduct, which can be difficult when platforms offer services "free" in exchange for data or when algorithmic practices are opaque.[81] Third, the ex-post nature of competition law enforcement means that by the time investigations are completed and remedies imposed, market structures may have become entrenched.[82] Fourth, penalties under the Competition Act, while higher than under the CPA 2019 (up to 10% of average turnover for three preceding financial years), have been criticized as insufficient to deter violations by large multinational corporations.[83]

The Committee on Digital Competition Law, established by the Ministry of Corporate Affairs in 2024, recommended enacting digital markets-specific legislation to address these challenges.[84] The Committee proposed an ex-ante regulatory framework that would designate "Systemically Significant Digital Enterprises" (SSDEs) based on quantitative thresholds (turnover, market capitalization, number of users) and qualitative factors (gatekeeper position, data advantages, network effects).[85] SSDEs would be subject to specific obligations including non-discrimination, interoperability, data portability, transparency in ranking and search, and prohibitions on self-preferencing and tying.[86] The proposed framework draws inspiration from the European Union's Digital Markets Act while adapting to Indian market conditions and regulatory capacity.[87]

C. Digital Personal Data Protection Act, 2023: The Privacy Dimension

The Digital Personal Data Protection Act, 2023 (DPDPA 2023) establishes a comprehensive framework for processing personal data, with significant implications for unfair trade practices

[79] Competition Commission of India, META-WHATSAPP PRIVACY POLICY INVESTIGATION (2021) (India).
[80] *Supra* note 3.
[81] *Id.*
[82] *Supra* note 9.
[83] *Id.*
[84] *Supra* note 11.
[85] *Id.*
[86] *Id.*
[87] *Id.*

 [ISSN 2581-5369]

in digital markets.[88] The Act is based on principles of consent, purpose limitation, data minimization, accuracy, storage limitation, and reasonable security safeguards.[89] Section 6 requires data fiduciaries to obtain consent from data principals before processing personal data, with consent required to be free, specific, informed, unconditional, and unambiguous.[90] Section 7 provides data principals with rights including the right to access information about personal data processed, the right to correction and erasure, the right to grievance redressal, and the right to nominate another individual to exercise rights in the event of death or incapacity.[91]

Section 8 imposes general obligations on data fiduciaries including: (a) processing personal data in a lawful, fair, and transparent manner; (b) ensuring completeness, accuracy, and consistency of personal data; (c) implementing appropriate technical and organizational measures to ensure effective observance of the Act; (d) implementing appropriate technical and organizational measures to implement security safeguards; (e) notifying the Data Protection Board and affected data principals of personal data breaches; (f) erasing personal data when retention is no longer necessary for the specified purpose; and (g) publishing information about personal data processed, the purpose of processing, and the manner in which data principals may exercise their rights.[92]

Section 9 designates certain data fiduciaries as "Significant Data Fiduciaries" based on factors including volume and sensitivity of personal data processed, risk to rights of data principals, potential impact on sovereignty and integrity of India, risk to electoral democracy, security of the State, and public order.[93] Significant Data Fiduciaries are subject to additional obligations including appointing a Data Protection Officer, conducting Data Protection Impact Assessments, conducting periodic audits, and undertaking such other measures as may be prescribed.[94]

The DPDPA 2023 has important implications for unfair trade practices in digital markets. First, the consent requirements limit platforms' ability to engage in unfair data collection practices, though the effectiveness depends on how "free" and "informed" consent is interpreted and enforced.[95] Second, the transparency obligations require platforms to disclose how personal data is processed, potentially reducing information asymmetries that enable unfair practices.[96]

[88] *Supra* note 8.
[89] *Id.* § 4.
[90] *Id.* § 6.
[91] *Id.* § 7.
[92] *Id.* § 8.
[93] *Id.* § 9.
[94] *Id.*
[95] *Supra* note 33.
[96] *Supra* note 8, § 8.

 [ISSN 2581-5369]

Third, the data portability provisions (to be specified in rules) could reduce switching costs and promote competition, though implementation challenges remain.[97] Fourth, the prohibition on processing personal data in a manner that is likely to cause harm to data principals could encompass manipulative practices like behavioural targeting and algorithmic discrimination.[98]

However, scholars have identified several limitations. First, the Act's consent-based framework may be inadequate for addressing structural power imbalances in digital markets, where consumers have little choice but to accept platforms' terms.[99] Second, the Act does not explicitly address dark patterns in obtaining consent, though the requirement that consent be "free" and "unambiguous" could be interpreted to prohibit such practices.[100] Third, the Act's enforcement mechanisms and penalty provisions (up to Rs. 250 crore for violations) remain to be tested in practice.[101] Fourth, coordination between the Data Protection Board, CCI, and CCPA will be critical to avoid regulatory gaps and overlaps.[102]

D. Regulatory Harmonization Challenges

India's regulatory architecture for digital markets involves multiple authorities with overlapping jurisdictions: the Central Consumer Protection Authority under the Ministry of Consumer Affairs, the Competition Commission of India under the Ministry of Corporate Affairs, the Data Protection Board under the Ministry of Electronics and Information Technology, and sectoral regulators like the Telecom Regulatory Authority of India and the Reserve Bank of India for specific industries.[103] This fragmentation creates several challenges.

First, definitional inconsistencies across legal frameworks create uncertainty. The CPA 2019, Competition Act 2002, and DPDPA 2023 use different definitions for key concepts like "consumer," "unfair practice," and "harm," potentially leading to inconsistent interpretations and enforcement.[104] Second, overlapping jurisdictions can result in duplicative investigations, conflicting decisions, and forum shopping by regulated entities.[105] Third, coordination mechanisms between authorities remain underdeveloped, with no formal framework for joint investigations, information sharing, or coordinated enforcement actions.[106] Fourth, resource

[97] *Id.* § 7.
[98] *Id.* § 8.
[99] *Supra* note 33.
[100] *Id.*
[101] *Supra* note 8, § 33.
[102] *Supra* note 10.
[103] Reddy, Promotion and Regulation of E-Commerce in India, PARLIAMENT OF INDIA, RAJYA SABHA (2022).
[104] *Supra* note 10.
[105] *Id.*
[106] *Id.*

 [ISSN 2581-5369]

constraints affect all regulatory authorities, limiting their capacity to investigate complex digital market practices and enforce against well-resourced multinational corporations.[107]

Scholars have proposed several approaches to address these challenges. Some advocate for establishing a unified digital markets regulator with comprehensive authority over competition, consumer protection, and data privacy issues in digital markets.[108] Others propose maintaining separate authorities but strengthening coordination through memoranda of understanding, joint guidelines, and coordinated enforcement actions.[109] The Committee on Digital Competition Law recommended that the proposed digital competition legislation should include provisions for coordination with other regulatory authorities and that the CCI should have powers to refer matters to the CCPA or Data Protection Board when practices implicate multiple legal domains.[110]

IV. TAXONOMY OF UNFAIR TRADE PRACTICES IN DIGITAL MARKETS

A. Algorithmic Pricing and Discriminatory Strategies

Algorithmic pricing involves using automated systems to set prices based on real-time analysis of supply, demand, competitor pricing, and consumer characteristics.[111] While dynamic pricing itself is not necessarily unfair, algorithmic systems enable forms of price discrimination and manipulation that raise legal and ethical concerns.[112] Personalized pricing, where different consumers are charged different prices for identical goods or services based on their willingness to pay, exploits information asymmetries and can constitute unfair trade practice when it discriminates against vulnerable consumers or lacks transparency.[113]

Algorithmic collusion occurs when pricing algorithms learn to coordinate without explicit agreement among competitors, resulting in supra-competitive prices.[114] Unlike traditional cartels, algorithmic collusion may occur without human intent or communication, raising novel questions about liability and enforcement under competition law.[115] The Samir Agarwal v. CCI case in India highlighted the challenges of detecting and proving algorithmic collusion in the airline industry, where parallel pricing patterns may result from algorithmic coordination or

[107] *Supra* note 9.
[108] *Supra* note 11.
[109] *Supra* note 10.
[110] *Supra* note 11.
[111] *Supra* note 2.
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] *Id.*

 [ISSN 2581-5369]

legitimate responses to market conditions.[116]

Surge pricing in ride-hailing and food delivery platforms has been criticized as exploitative when it occurs during emergencies or when consumers have limited alternatives.[117] While platforms argue that surge pricing balances supply and demand, consumer advocates contend that it exploits consumer vulnerability and lacks sufficient transparency about how prices are calculated.[118] The CCPA has investigated complaints about excessive surge pricing during the COVID-19 pandemic, though no final orders have been issued.[119]

Drip pricing, where additional charges are revealed incrementally during the purchase process, is explicitly prohibited under the CCPA's Dark Patterns Guidelines.[120] This practice is prevalent in online travel booking, event ticketing, and e-commerce, where base prices are advertised prominently but mandatory fees (service charges, convenience fees, delivery charges) are disclosed only at checkout.[121] Drip pricing exploits the endowment effect and sunk cost fallacy, making consumers more likely to complete purchases even when the final price exceeds their initial willingness to pay.[122]

Reference price manipulation involves displaying inflated "original" or "maximum retail" prices alongside discounted "sale" prices to create the perception of value.[123] The CCI has investigated e-commerce platforms for requiring sellers to maintain artificially high MRPs to enable deep discounting, which can mislead consumers and distort competition.[124] The Legal Metrology (Packaged Commodities) Rules, 2011 require that MRP reflect the actual maximum price at which goods are intended to be sold, but enforcement in e-commerce contexts remains limited.[125]

B. Dark Patterns: Interface-Based Deception

Dark patterns are user interface designs that manipulate users into making choices they would not otherwise make, exploiting cognitive biases and bounded rationality.[126] The CCPA's 2023

[116] *Id.*
[117] Kumar et al., Fair and Competitive E-Marketplaces (F.A.C.E.) | The Business Users' Narrative (2021) (Working Paper).
[118] *Id.*
[119] *Supra* note 49.
[120] *Supra* note 6.
[121] *Id.*
[122] Raj et al., Safeguarding the Digital Consumer: A Comparative Legal and Psychological Analysis of Dark Patterns in E-Commerce (2024).
[123] *Supra* note 7.
[124] *Id.*
[125] Legal Metrology (Packaged Commodities) Rules, 2011 (India).
[126] *Supra* note 32.

 [ISSN 2581-5369]

Guidelines identify thirteen categories of dark patterns, reflecting growing regulatory attention to interface-based manipulation.[127]

False urgency creates artificial time pressure through countdown timers, limited stock warnings, or claims that deals will expire soon, even when these claims are false or misleading.[128] This practice exploits scarcity bias and fear of missing out (FOMO), pressuring consumers to make hasty decisions without adequate deliberation.[129] The CCPA issued notices to IndiGo Airlines for using false urgency tactics in its booking interface, marking one of the first enforcement actions under the Dark Patterns Guidelines.[130]

Basket sneaking involves adding items to a consumer's shopping cart without explicit consent, such as insurance, extended warranties, or donation requests that are pre-selected by default.[131] This practice exploits inertia and the default effect, as consumers are more likely to accept pre-selected options than to actively opt out.[132] The practice is particularly problematic when the added items are difficult to identify or remove, or when they are presented as mandatory when they are actually optional.[133]

Confirm shaming uses emotionally manipulative language to discourage users from declining offers or opting out of services.[134] Examples include "No thanks, I don't want to save money" or "No, I prefer to pay full price" as opt-out options, which shame users for making economically rational choices.[135] This practice exploits social norms and self-image concerns, making users feel guilty or foolish for declining offers.[136]

Forced action requires users to perform unrelated actions (such as sharing personal information, creating accounts, or subscribing to newsletters) as a condition for accessing desired services.[137] This practice is particularly problematic when the forced action involves sharing personal data that is not necessary for the service, potentially violating data minimization principles under the DPDPA 2023.[138]

Subscription traps make it easy to subscribe but difficult to cancel, using complex cancellation

[127] *Supra* note 6.
[128] *Id.*
[129] *Supra* note 121.
[130] *Supra* note 49.
[131] *Supra* note 6.
[132] *Supra* note 121.
[133] *Supra* note 6.
[134] *Id.*
[135] *Id.*
[136] *Supra* note 121.
[137] *Supra* note 6.
[138] *Supra* note 8, § 4.

 [ISSN 2581-5369]

processes, hidden cancellation options, or requiring phone calls or written requests to cancel online subscriptions.[139] This practice exploits inertia and transaction costs, leading consumers to maintain subscriptions they no longer want rather than navigate burdensome cancellation processes.[140] The practice may violate the CPA 2019's prohibition on unfair contract terms and the DPDPA 2023's requirement that consent be freely given.[141]

Interface interference involves manipulating the visual design or information architecture to steer users toward certain choices, such as making preferred options more prominent, using confusing layouts, or obscuring important information.[142] This includes practices like making "accept" buttons large and colourful while making "decline" buttons small and grey, or burying privacy-protective options in complex settings menus.[143]

C. Deceptive Marketing and Advertising Practices

False and misleading advertisements in digital markets take forms that differ from traditional media advertising. Native advertising and sponsored content blur the line between editorial content and advertising, potentially misleading consumers about the commercial nature of content.[144] The Advertising Standards Council of India (ASCI) has issued guidelines requiring clear disclosure of sponsored content, but enforcement remains inconsistent.[145]

Influencer marketing raises concerns about non-disclosure of commercial relationships between brands and influencers.[146] The ASCI's Influencer Advertising Guidelines require influencers to disclose material connections with brands using clear labels like "ad," "sponsored," or "paid partnership," but compliance is limited and enforcement mechanisms are weak.[147] The CPA 2019 makes endorsers liable for false or misleading advertisements, but few cases have been brought against influencers.[148]

Fake reviews, paid ratings, and astroturfing undermine the reliability of user-generated content that consumers rely on for purchase decisions.[149] The Consumer Protection (E-Commerce) Rules, 2020 prohibit e-commerce entities from manipulating reviews or suppressing negative

[139] *Supra* note 6.
[140] *Supra* note 121.
[141] *Supra* note 35, § 2(47); *supra* note 8, § 6.
[142] *Supra* note 6.
[143] *Id.*
[144] Advertising Standards Council of India, GUIDELINES FOR INFLUENCER ADVERTISING IN DIGITAL MEDIA (2021).
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Supra* note 35, § 21.
[149] *Supra* note 57, r. 6.

 [ISSN 2581-5369]

reviews, but detecting and proving such manipulation is challenging.[150] The CCPA has issued notices to platforms for failing to prevent fake reviews, but systematic enforcement remains limited.[151]

Greenwashing involves making false or misleading claims about environmental benefits of products or services.[152] Digital platforms enable sophisticated greenwashing through selective disclosure, vague claims, and misleading imagery.[153] The Bureau of Indian Standards has developed standards for environmental claims, but enforcement in digital contexts is limited.[154]

Image editing and digital manipulation can create false impressions about product characteristics, particularly in fashion, beauty, and food categories.[155] While some degree of image enhancement is accepted, practices that materially misrepresent products may constitute unfair trade practices under the CPA 2019.[156] The Legal Metrology Act requires that packaged commodities display accurate information, but application to digital product images remains ambiguous.[157]

D. Data Exploitation and Privacy Violations as Unfair Trade Practices

Unfair data collection practices include collecting personal data without adequate consent, collecting more data than necessary for the stated purpose, or using dark patterns to obtain consent.[158] The DPDPA 2023 requires that consent be free, specific, informed, unconditional, and unambiguous, but enforcement will depend on how these requirements are interpreted and applied.[159] Practices like pre-checked consent boxes, bundled consent for multiple purposes, or consent obtained through confusing interfaces may violate these requirements.[160]

Hidden data monetization occurs when platforms offer "free" services while generating revenue through data collection and targeted advertising, without adequately disclosing this economic model to users.[161] This creates information asymmetry about the true costs of platform participation and may constitute unfair trade practice when the value extracted through data monetization substantially exceeds the value of services provided.[162] The "free" service model

[150] *Id.*
[151] *Supra* note 49.
[152] Bureau of Indian Standards, STANDARDS FOR ENVIRONMENTAL CLAIMS (2023).
[153] *Id.*
[154] *Id.*
[155] *Supra* note 49.
[156] *Supra* note 35, § 2(47).
[157] *Supra* note 124.
[158] *Supra* note 33.
[159] *Supra* note 8, § 6.
[160] *Supra* note 33.
[161] *Supra* note 4.
[162] *Id.*

 [ISSN 2581-5369]

obscures the economic exchange, making it difficult for consumers to make informed decisions about platform participation.[163]

behavioural targeting and profiling enable platforms to manipulate consumer behaviour through personalized content, recommendations, and advertisements.[164] While personalization can benefit consumers by showing relevant content, it can also exploit vulnerabilities, reinforce biases, and manipulate decision-making.[165] Algorithmic amplification of engagement-maximizing content can expose users to harmful or misleading information, raising questions about platform responsibility.[166]

Data sharing with third parties without adequate disclosure or consent is prohibited under the DPDPA 2023, but enforcement challenges remain.[167] Complex data ecosystems involving multiple intermediaries, data brokers, and advertising networks make it difficult for consumers to understand how their data is shared and used.[168] The Meta-WhatsApp privacy policy controversy highlighted concerns about data sharing within corporate groups and the adequacy of consent mechanisms.[169]

E. Platform-to-Business Unfair Practices

Self-preferencing occurs when vertically integrated platforms favour their own products or services over those of competitors using the platform.[170] The Amazon-Flipkart investigation examined allegations that these platforms used seller data to launch competing private label products and gave preferential treatment to their own brands in search rankings and promotions.[171] Self-preferencing can foreclose competition, reduce innovation, and harm consumers by limiting choice and increasing prices.[172]

Unfair contract terms in platform-to-business relationships include unilateral modification clauses, excessive liability limitations, mandatory arbitration clauses, and non-compete provisions.[173] Small and medium enterprises often have no choice but to accept these terms to access platform markets, creating significant power imbalances.[174] The Competition Act's

[163] *Id.*
[164] Chauhan et al., Darker Patterns? AI-Generated Persuasion and the Regulatory Void in Indian Law, J. OF DEV. POL'Y & PRACTICE (2024), https://doi.org/10.1177/24551333241275752.
[165] *Id.*
[166] *Id.*
[167] *Supra* note 8, § 8.
[168] *Supra* note 4.
[169] *Supra* note 78.
[170] *Supra* note 7.
[171] *Id.*
[172] *Id.*
[173] *Supra* note 116.
[174] *Id.*

 [ISSN 2581-5369]

prohibition on abuse of dominance could apply to unfair contract terms imposed by dominant platforms, though enforcement has been limited.[175]

Opaque ranking and search algorithms make it difficult for business users to understand how to optimize their visibility on platforms.[176] Platforms may manipulate rankings to favour certain sellers, extract higher commissions, or promote their own products, without disclosing these practices to business users or consumers.[177] The Consumer Protection (E-Commerce) Rules, 2020 prohibit manipulation of search results but do not require disclosure of ranking algorithms.[178]

Excessive commissions and fees have been challenged by business users as exploitative, particularly when platforms hold dominant positions and business users have limited alternatives.[179] The Google Play Store billing case examined whether Google's requirement that app developers use its payment system and pay 15-30% commissions constituted abuse of dominance.[180] The CCI found that Google's practices violated Section 4 of the Competition Act and ordered remedial measures.[181]

Data exploitation in platform-to-business relationships occurs when platforms use data generated by business users to compete against them or to extract rents.[182] Platforms have privileged access to marketplace data including sales volumes, pricing strategies, and customer preferences, which they can leverage for competitive advantage.[183] The proposed digital competition legislation includes provisions to address such data-related unfair practices.[184]

V. ENFORCEMENT CHALLENGES: THE MULTINATIONAL CORPORATION ACCOUNTABILITY GAP

A. Complex Corporate Structures and Jurisdictional Fragmentation

Multinational digital corporations employ complex corporate structures involving multiple subsidiaries, holding companies, and special purpose vehicles across different jurisdictions, making it difficult to establish accountability and enforce regulatory decisions.[185] Indian

[175] *Supra* note 34, § 4.
[176] *Supra* note 116.
[177] *Id.*
[178] *Supra* note 57, r. 5.
[179] *Supra* note 77.
[180] *Id.*
[181] *Id.*
[182] *Supra* note 7.
[183] *Id.*
[184] *Supra* note 11.
[185] *Supra* note 7.

operations are often conducted through local subsidiaries with limited assets and decision-making authority, while key functions like algorithm development, data processing, and strategic decisions are controlled by foreign parent companies.[186] This structure enables corporations to argue that Indian regulators lack jurisdiction over foreign entities, even when those entities control the practices that harm Indian consumers.[187]

The Amazon-Flipkart investigation revealed how complex corporate structures can obscure accountability. Amazon operates in India through multiple entities including Amazon Seller Services (marketplace), Amazon Wholesale India (B2B), Amazon Pay India (payments), and Amazon Transportation Services (logistics), each with distinct legal status and functions.[188] When the CCI sought information about Amazon's global practices and decision-making, Amazon argued that Indian subsidiaries are independent entities and that the CCI lacks jurisdiction over Amazon.com Inc.[189] Similar jurisdictional challenges have arisen in cases involving Google, Meta, and other multinational platforms.[190]

Regulatory arbitrage occurs when corporations structure operations to take advantage of differences in regulatory regimes across jurisdictions.[191] Data may be processed in jurisdictions with weak data protection laws, intellectual property may be held in tax havens, and key decisions may be made in jurisdictions with limited regulatory oversight.[192] The DPDPA 2023 includes extraterritorial provisions applying to processing of personal data of individuals in India, but enforcement against foreign entities remains challenging.[193]

B. Resource Asymmetries and Strategic Litigation

Resource asymmetries between multinational corporations and Indian regulatory authorities create significant enforcement challenges. Major digital platforms have legal budgets exceeding the entire annual budgets of regulatory authorities, enabling them to employ large teams of lawyers, economists, and technical experts to contest regulatory actions.[194] The CCI, CCPA, and Data Protection Board face budgetary and staffing constraints that limit their capacity to investigate complex digital market practices and litigate against well-resourced corporations.[195]

Strategic litigation tactics employed by multinational corporations include: filing multiple

[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] *Supra* note 77; *supra* note 78.
[191] *Supra* note 47.
[192] *Id.*
[193] *Supra* note 8, § 2.
[194] *Supra* note 9.
[195] *Id.*

appeals and writ petitions to delay enforcement; challenging regulatory jurisdiction and authority; demanding extensive discovery and procedural rights; and threatening to exit the Indian market or reduce investment.[196] These tactics can delay final resolution of cases for years, during which time harmful practices continue and market structures become further entrenched.[197]

The Meta-WhatsApp privacy policy case illustrates these challenges. After the CCI issued a show cause notice in 2021, Meta filed multiple legal challenges questioning the CCI's jurisdiction, arguing that the matter should be handled by the Data Protection Authority (which did not yet exist), and contesting the CCI's information requests.[198] As of 2025, the case remains pending, with no final order issued despite widespread concerns about the privacy policy's impact on Indian users.[199]

Technical expertise gaps compound resource asymmetries. Investigating algorithmic practices, data processing systems, and platform architectures requires specialized technical knowledge that regulatory authorities often lack.[200] While the CCI has established a Digital Markets and Data Unit and the CCPA has hired technical experts, capacity remains limited compared to the sophisticated technical and legal teams employed by platforms.[201] The proposed digital competition legislation includes provisions for the CCI to hire technical experts and consultants, but implementation will depend on adequate funding.[202]

C. Cross-Border Data Flows and Regulatory Circumvention

Cross-border data flows enable platforms to process Indian users' data in foreign jurisdictions, potentially circumventing Indian data protection and consumer protection laws.[203] While the DPDPA 2023 includes provisions for cross-border data transfers, these are subject to conditions and restrictions that remain to be specified in rules.[204] Platforms may argue that data processing occurs outside India and therefore falls outside Indian regulatory jurisdiction, even when the data relates to Indian users and the processing affects Indian markets.[205]

The lack of data localization requirements in the DPDPA 2023 (unlike earlier draft bills) has

[196] *Supra* note 7.
[197] *Id.*
[198] *Supra* note 78.
[199] *Id.*
[200] *Supra* note 9.
[201] *Id.*
[202] *Supra* note 11.
[203] *Supra* note 8, § 16.
[204] *Id.*
[205] *Id.*

 [ISSN 2581-5369]

been criticized as weakening enforcement capacity.[206] Without data localization, Indian authorities may face difficulties accessing data necessary for investigations, particularly when foreign jurisdictions do not cooperate or when platforms invoke foreign privacy laws to resist disclosure.[207] The DPDPA 2023 includes provisions for the Data Protection Board to request information from data fiduciaries, but enforcement against foreign entities remains uncertain.[208]

Mutual Legal Assistance Treaties (MLATs) and other international cooperation mechanisms are often slow and cumbersome, making them inadequate for addressing fast-moving digital market practices.[209] India has MLATs with several countries, but these are primarily designed for criminal matters and may not cover regulatory investigations.[210] The proposed digital competition legislation includes provisions for international cooperation, but effectiveness will depend on reciprocal arrangements with other jurisdictions.[211]

D. Penalty Inadequacy and Deterrence Failures

Penalties imposed on multinational corporations for unfair trade practices and competition law violations have been criticized as insufficient to deter violations.[212] Under the CPA 2019, maximum penalties for unfair trade practices are Rs. 10 lakh for first violations and Rs. 50 lakh for subsequent violations amounts that are trivial compared to the revenues of major platforms.[213] Under the Competition Act, penalties can reach 10% of average turnover for three preceding financial years, but calculating turnover for multinational corporations with complex structures is challenging.[214]

The Google Android case resulted in a penalty of Rs. 1,337 crore (approximately USD 161 million), the largest competition penalty in Indian history.[215] However, this amount represents less than 1% of Google's annual revenue from India and a tiny fraction of Alphabet Inc.'s global revenue, raising questions about deterrent effect.[216] Google has appealed the decision and obtained stays on certain remedial measures, further delaying implementation.[217]

Scholars have proposed several reforms to enhance deterrence. First, penalties should be

[206] *Supra* note 33.
[207] *Id.*
[208] *Supra* note 8, § 28.
[209] *Supra* note 47.
[210] *Id.*
[211] *Supra* note 11.
[212] *Supra* note 9.
[213] *Supra* note 35, § 21.
[214] *Supra* note 34, § 27.
[215] *Supra* note 77.
[216] *Supra* note 9.
[217] *Supra* note 77.

 [ISSN 2581-5369]

calculated based on global turnover rather than Indian turnover, reflecting the integrated nature of multinational corporations and preventing artificial separation of Indian operations.[218] Second, penalties should include aggravating factors for repeat violations, obstruction of investigations, and failure to implement remedial measures.[219] Third, disgorgement of ill-gotten gains should be available as a remedy, ensuring that violations are not profitable even after penalties.[220] Fourth, personal liability for executives and directors should be considered for egregious violations, as provided in the DPDPA 2023.[221]

VI. COMPARATIVE ANALYSIS: GLOBAL REGULATORY APPROACHES

A. European Union: Digital Markets Act and Digital Services Act

The European Union has adopted a comprehensive regulatory framework for digital markets through the Digital Markets Act (DMA) and Digital Services Act (DSA), representing the most ambitious ex-ante regulation of digital platforms globally.[222] The DMA, which entered into force in November 2022 and became applicable in May 2023, establishes obligations for "gatekeepers" large platforms that provide core platform services and hold entrenched and durable positions.[223]

Article 3 of the DMA establishes quantitative thresholds for gatekeeper designation: annual EEA turnover of at least €7.5 billion or market capitalization of at least €75 billion, provision of core platform services in at least three EU member states, and at least 45 million monthly active end users and 10,000 yearly active business users in the EU.[224] The European Commission has designated six gatekeepers (Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft) covering 22 core platform services.[225]

Articles 5 and 6 of the DMA impose obligations on gatekeepers including: prohibitions on combining personal data from different services without consent; prohibitions on using data generated by business users to compete against them; requirements to allow business users to offer different prices or conditions through other channels; requirements for interoperability of messaging services; requirements to allow uninstallation of pre-installed apps; prohibitions on self-preferencing; and requirements for fair and non-discriminatory access to app stores.[226]

[218] *Supra* note 9.
[219] *Id.*
[220] *Id.*
[221] *Supra* note 8, § 33.
[222] *Supra* note 29.
[223] *Id.* art. 2.
[224] *Id.* art. 3.
[225] European Commission, DESIGNATION DECISIONS UNDER THE DIGITAL MARKETS ACT (2024).
[226] *Supra* note 29, arts. 5–6.

 [ISSN 2581-5369]

Article 30 provides for penalties up to 10% of worldwide turnover for violations, with enhanced penalties up to 20% for repeated infringements.[227]

The Digital Services Act, which entered into force in November 2022 and became fully applicable in February 2024, establishes a comprehensive framework for platform liability, content moderation, and transparency.[228] Article 33 prohibits dark patterns in online interfaces, requiring that platforms design interfaces in a way that does not deceive or manipulate users.[229] Articles 25-27 impose transparency obligations on recommender systems and online advertising, requiring platforms to disclose the main parameters used in recommender systems and to provide users with options to modify or influence those parameters.[230]

The EU approach offers several lessons for India. First, ex-ante regulation can address structural issues in digital markets more effectively than ex-post enforcement, particularly for entrenched platforms where remedies may be too late to restore competition.[231] Second, clear quantitative thresholds for designation provide legal certainty while qualitative factors allow flexibility to address evolving market dynamics.[232] Third, comprehensive obligations addressing multiple dimensions of platform conduct (data practices, self-preferencing, interoperability, transparency) are necessary to address the multifaceted nature of digital market power.[233] Fourth, substantial penalties linked to global turnover are necessary to deter violations by large multinational corporations.[234]

However, the EU approach also faces challenges relevant to India. Implementation requires substantial regulatory capacity, including technical expertise to assess compliance with complex obligations like interoperability and data portability.[235] Gatekeepers have challenged various aspects of the DMA, including gatekeeper designations and specific obligations, leading to ongoing litigation.[236] The effectiveness of the DMA in promoting competition and innovation will take years to assess, as structural changes in digital markets occur slowly.[237]

[227] *Id.* art. 30.
[228] Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act).
[229] *Id.* art. 33.
[230] *Id.* arts. 25–27.
[231] *Supra* note 9.
[232] *Supra* note 11.
[233] *Id.*
[234] *Supra* note 9.
[235] *Supra* note 11.
[236] *Supra* note 224.
[237] *Supra* note 9.

 [ISSN 2581-5369]

B. United Kingdom: Digital Markets Unit and Pro-Competition Regime

The United Kingdom has adopted a different approach through the Digital Markets, Competition and Consumers Act 2024, which establishes a pro-competition regime for digital markets administered by the Digital Markets Unit (DMU) within the Competition and Markets Authority (CMA).[238] Unlike the EU's DMA, which applies automatically to designated gatekeepers, the UK regime involves designation of firms with "Strategic Market Status" (SMS) in specific digital activities, followed by tailored conduct requirements and pro-competitive interventions.[239]

The SMS designation process involves the CMA conducting market investigations to determine whether a firm has substantial and entrenched market power and a position of strategic significance in a digital activity.[240] Factors considered include market share, barriers to entry and expansion, network effects, access to data, financial resources, and vertical integration.[241] Once designated, the CMA can impose conduct requirements tailored to the specific competition concerns in that market, including requirements for fair trading, open choices, trust and transparency, and fair dealing.[242]

The UK approach offers flexibility to address market-specific concerns through tailored interventions rather than applying uniform obligations across all designated firms.[243] This may be more appropriate for markets with heterogeneous competitive dynamics and may reduce the risk of over-regulation.[244] However, the approach also involves greater regulatory discretion and potentially longer timelines for designation and intervention, which may delay addressing harmful practices.[245]

The UK regime includes strong enforcement powers, with penalties up to 10% of global turnover for non-compliance with conduct requirements and up to 5% of global turnover for failure to provide information.[246] The CMA can also impose interim measures to prevent harm while investigations are ongoing.[247] These provisions address concerns about penalty inadequacy and enforcement delays that have plagued traditional competition law

[238] UK Digital Markets, Competition and Consumers Act 2024.
[239] *Id.*
[240] *Id.*
[241] *Id.*
[242] *Id.*
[243] UK Competition and Markets Authority, DIGITAL MARKETS UNIT (2021).
[244] *Id.*
[245] *Id.*
[246] *Supra* note 237.
[247] *Id.*

 [ISSN 2581-5369]

enforcement.[248]

C. United States: Antitrust Enforcement and Proposed Legislation

The United States has relied primarily on antitrust enforcement under existing laws (Sherman Act, Clayton Act, Federal Trade Commission Act) rather than adopting digital markets-specific legislation, though several bills have been proposed.[249] The Federal Trade Commission (FTC) and Department of Justice (DOJ) have brought major antitrust cases against digital platforms, including cases against Google (search and advertising, app store), Meta (acquisitions of Instagram and WhatsApp), Amazon (e-commerce and cloud services), and Apple (app store).[250]

The FTC's case against Meta challenges the acquisitions of Instagram (2012) and WhatsApp (2014) anti-competitive, arguing that Meta acquired potential competitors to maintain its monopoly in social networking.[251] The DOJ's case against Google challenges its agreements with device manufacturers and browsers to make Google the default search engine, arguing that these agreements foreclose competition and maintain Google's monopoly in search.[252] These cases represent a more aggressive approach to antitrust enforcement in digital markets than in previous decades, but outcomes remain uncertain and remedies may take years to implement.[253]

Several bills have been proposed to address digital market competition, though none have been enacted as of 2025. The American Innovation and Choice Online Act would prohibit self-preferencing and other discriminatory practices by covered platforms.[254] The Open App Markets Act would require app store operators to allow sideloading and alternative payment systems.[255] The Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act would require data portability and interoperability.[256] These bills face opposition from industry and concerns about unintended consequences, making enactment uncertain.[257]

The US approach demonstrates both the potential and limitations of relying on traditional antitrust enforcement for digital markets. Antitrust cases can address egregious conduct and

[248] *Supra* note 9.
[249] U.S. Federal Trade Commission & Department of Justice, ANTITRUST ENFORCEMENT IN DIGITAL MARKETS (2024).
[250] *Id.*
[251] FTC v. Facebook, Inc., No. 1:20-cv-03590 (D.D.C. filed Dec. 9, 2020).
[252] United States v. Google LLC, No. 1:20-cv-03010 (D.D.C. filed Oct. 20, 2020).
[253] *Supra* note 248.
[254] American Innovation and Choice Online Act, S. 2992, 117th Cong. (2022).
[255] Open App Markets Act, S. 2710, 117th Cong. (2022).
[256] Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, S. 2448, 117th Cong. (2021).
[257] *Supra* note 248.

potentially result in structural remedies (such as divestitures), but they are slow, resource-intensive, and uncertain in outcome.[258] The lack of ex-ante regulation means that harmful practices may continue for years while cases are litigated, and market structures may become entrenched before remedies are implemented.[259] However, the US approach avoids potential over-regulation and preserves flexibility to address evolving market dynamics through case-by-case adjudication.[260]

D. Lessons for India

Comparative analysis of global regulatory approaches yields several lessons for India. First, digital markets-specific legislation is necessary to address structural issues that traditional competition law and consumer protection frameworks cannot adequately address.[261] The EU's DMA and UK's pro-competition regime demonstrate that ex-ante regulation can complement ex-post enforcement, particularly for addressing entrenched market power and preventing harmful practices before they cause irreversible harm.[262]

Second, clear designation criteria combining quantitative thresholds and qualitative factors provide legal certainty while allowing flexibility to address evolving market dynamics.[263] India's proposed digital competition legislation should establish transparent criteria for designating Systemically Significant Digital Enterprises, drawing on the EU and UK experiences while adapting to Indian market conditions.[264]

Third, comprehensive obligations addressing multiple dimensions of platform conduct are necessary to address the multifaceted nature of digital market power.[265] Obligations should address data practices, self-preferencing, interoperability, transparency, and fair dealing, tailored to specific platform types and competitive concerns.[266]

Fourth, substantial penalties linked to global turnover are necessary to deter violations by large multinational corporations.[267] India should consider penalties up to 10% of global turnover for violations, with enhanced penalties for repeat violations and obstruction of investigations, as provided in the EU DMA and UK regime.[268]

---

[258] *Id.*
[259] *Id.*
[260] *Id.*
[261] *Supra* note 11.
[262] *Id.*
[263] *Id.*
[264] *Id.*
[265] *Id.*
[266] *Id.*
[267] *Supra* note 9.
[268] *Supra* note 29, art. 30; *supra* note 237.

 [ISSN 2581-5369]

Fifth, regulatory capacity and technical expertise are critical for effective implementation.[269] India should invest in building capacity within the CCI, CCPA, and Data Protection Board, including hiring technical experts, developing analytical tools, and providing continuous training.[270] International cooperation and knowledge sharing can help build capacity and learn from other jurisdictions' experiences.[271]

Sixth, coordination between regulatory authorities is essential to address practices that implicate multiple legal domains.[272] India should establish formal coordination mechanisms including joint guidelines, information sharing protocols, and coordinated enforcement actions, drawing on models like the EU's Digital Services Coordinator and Digital Markets Coordinator.[273]

VII. POLICY RECOMMENDATIONS AND LEGAL REFORM PROPOSALS

A. Enact Digital Markets-Specific Legislation

India should enact comprehensive digital markets legislation based on the Committee on Digital Competition Law's recommendations, establishing an ex-ante regulatory framework for Systemically Significant Digital Enterprises (SSDEs).[274] The legislation should include:

Designation criteria: Quantitative thresholds based on turnover (e.g., Rs. 4,000 crore annual India turnover or Rs. 16,000 crore market capitalization), user base (e.g., 10 million active business users or 1 crore active end users in India), and qualitative factors including gatekeeper position, network effects, data advantages, vertical integration, and dependence of business users.[275]

Core obligations: Prohibitions on self-preferencing, tying, and bundling; requirements for data portability and interoperability; transparency obligations for ranking algorithms and recommender systems; fair and non-discriminatory access to platform services; prohibitions on using business user data to compete against them; and requirements to allow business users to offer different terms through other channels.[276]

Enforcement mechanisms: Penalties up to 10% of global turnover for violations, with enhanced penalties up to 20% for repeat violations; interim measures to prevent harm during investigations; structural remedies including divestiture for egregious or repeated violations;

[269] *Supra* note 11.
[270] *Id.*
[271] *Id.*
[272] *Supra* note 10.
[273] *Supra* note 227, arts. 49–50.
[274] *Supra* note 11.
[275] *Id.*
[276] *Id.*

 [ISSN 2581-5369]

and personal liability for executives who knowingly authorize violations.[277]

Procedural safeguards: Clear timelines for designation decisions and compliance assessments; opportunities for designated firms to propose compliance measures; and appeal mechanisms to specialized tribunals with technical expertise.[278]

B. Strengthen Consumer Protection Enforcement

The Consumer Protection Act, 2019 and Consumer Protection (E-Commerce) Rules, 2020 should be amended to enhance enforcement against unfair trade practices in digital markets:

Enhanced penalties: Increase maximum penalties to Rs. 100 crore or 2% of turnover (whichever is higher) for unfair trade practices, with enhanced penalties for repeat violations and violations affecting vulnerable consumers.[279] Link penalties to harm caused and benefits obtained from violations, including disgorgement of ill-gotten gains.[280]

Algorithmic transparency: Require platforms to disclose material information about algorithmic systems used for pricing, ranking, recommendations, and content moderation, including main parameters, data sources, and testing methodologies.[281] Establish algorithmic auditing requirements for high-risk systems affecting consumer rights.[282]

Dark patterns enforcement: Strengthen enforcement of the CCPA's Dark Patterns Guidelines through regular audits, mystery shopping, and user complaint mechanisms.[283] Establish a public registry of dark patterns violations and enforcement actions to increase transparency and accountability.[284]

Collective redress: Establish effective collective redress mechanisms for consumer harm in digital markets, including class actions and representative actions by consumer organizations.[285] Provide for statutory damages for certain violations to reduce barriers to litigation.[286]

C. Enhance Competition Law Enforcement Capacity

The Competition Commission of India should be provided with enhanced resources and powers to address digital market competition concerns:

---

[277] *Id.*
[278] *Id.*
[279] *Supra* note 9.
[280] *Id.*
[281] *Supra* note 11.
[282] *Id.*
[283] *Supra* note 6.
[284] *Supra* note 9.
[285] *Id.*
[286] *Id.*

 [ISSN 2581-5369]

Institutional capacity: Substantially increase the CCI's budget and staffing, with dedicated resources for the Digital Markets and Data Unit.[287] Hire technical experts including data scientists, algorithm specialists, and platform economists.[288] Provide continuous training on digital market dynamics and investigative techniques.[289]

Investigative powers: Enhance the CCI's powers to access data and information from platforms, including source code, algorithms, and internal communications.[290] Establish expedited procedures for obtaining information from foreign entities and parent companies.[291] Provide for penalties for obstruction of investigations and failure to provide information.[292]

Interim measures: Strengthen the CCI's powers to impose interim measures to prevent irreversible harm during investigations, with clear standards and expedited procedures.[293] Interim measures should be available for both abuse of dominance and anti-competitive agreements cases.[294]

Market studies: Expand the CCI's market study powers to conduct proactive investigations of digital markets, identifying competition concerns and recommending regulatory interventions.[295] Market studies should inform designation decisions under the proposed digital competition legislation.[296]

D. Harmonize Data Protection, Consumer Protection, and Competition Law

Establish formal coordination mechanisms between the Data Protection Board, Central Consumer Protection Authority, and Competition Commission of India:

Joint guidelines: Develop joint interpretive guidelines addressing practices that implicate multiple legal domains, including data-related competition concerns, dark patterns in consent mechanisms, and unfair contract terms regarding data processing.[297] Guidelines should clarify jurisdictional boundaries and coordination procedures.[298]

Information sharing: Establish protocols for sharing information and evidence between

[287] *Supra* note 11.
[288] *Id.*
[289] *Id.*
[290] *Id.*
[291] *Id.*
[292] *Id.*
[293] *Id.*
[294] *Id.*
[295] *Id.*
[296] *Id.*
[297] *Supra* note 10.
[298] *Id.*

 [ISSN 2581-5369]

authorities, subject to confidentiality protections.[299] Authorities should be able to refer matters to each other when practices implicate multiple legal domains.[300]

Coordinated enforcement: Develop procedures for coordinated investigations and enforcement actions when practices violate multiple legal frameworks.[301] Coordination should avoid duplicative proceedings while ensuring comprehensive remedies.[302]

Aligned definitions: Harmonize definitions of key concepts including "consumer," "unfair practice," "harm," and "consent" across legal frameworks to reduce inconsistencies and legal uncertainty.[303]

E. Strengthen Cross-Border Enforcement Mechanisms

Enhance India's capacity to enforce against multinational corporations through cross-border cooperation:

International agreements: Negotiate bilateral and multilateral agreements for regulatory cooperation, information sharing, and mutual recognition of enforcement decisions.[304] Agreements should cover both competition law and consumer protection enforcement.[305]

Extraterritorial jurisdiction: Clarify and strengthen extraterritorial jurisdiction provisions in Indian laws, ensuring that foreign entities affecting Indian markets and consumers are subject to Indian regulation.[306] Establish clear nexus requirements and service of process mechanisms.[307]

Global turnover penalties: Calculate penalties based on global turnover rather than Indian turnover for multinational corporations, reflecting their integrated operations and preventing artificial separation of Indian subsidiaries.[308]

Enforcement cooperation: Participate in international enforcement networks and working groups to share best practices, coordinate investigations, and develop common approaches to digital market regulation.[309]

---

[299] *Id.*
[300] *Id.*
[301] *Id.*
[302] *Id.*
[303] *Id.*
[304] *Supra* note 11.
[305] *Id.*
[306] *Id.*
[307] *Id.*
[308] *Id.*
[309] *Id.*

 [ISSN 2581-5369]

F. Promote Consumer Empowerment and Digital Literacy

Regulatory enforcement should be complemented by consumer empowerment initiatives:

Digital literacy programs: Develop comprehensive digital literacy programs educating consumers about unfair trade practices, privacy rights, and complaint mechanisms.[310] Programs should target vulnerable populations including rural consumers, elderly users, and low-income groups.[311]

Transparency tools: Require platforms to provide user-friendly transparency tools showing how personal data is collected and used, how algorithms affect content and pricing, and how to exercise consumer rights.[312] Tools should be accessible, understandable, and actionable.[313]

Complaint mechanisms: Establish accessible complaint mechanisms for reporting unfair trade practices, with clear procedures and timelines for resolution.[314] Complaints should be tracked and analysed to identify systemic issues requiring regulatory intervention.[315]

Consumer organizations: Support consumer organizations through funding, capacity building, and legal standing to bring representative actions.[316] Consumer organizations should be consulted in regulatory policy development.[317]

VIII. CONCLUSION

A. Summary of Key Findings

This article has demonstrated that unfair trade practices in India's digital economy are systematic patterns arising from structural asymmetries inherent in platform-based ecosystems, rather than isolated incidents of misconduct. Digital markets are characterized by network effects, data advantages, economies of scale, and multi-sided market structures that create conditions for market concentration and enable dominant platforms to engage in practices that harm consumers and smaller market participants. These practices include algorithmic manipulation and discriminatory pricing, dark patterns that exploit cognitive biases, deceptive marketing and advertising, data exploitation and privacy violations, and platform-to-business unfair practices including self-preferencing and unfair contract terms.

India's legal framework for addressing unfair trade practices in digital markets comprises the

[310] *Id.*
[311] *Id.*
[312] *Id.*
[313] *Id.*
[314] *Id.*
[315] *Id.*
[316] *Id.*
[317] *Id.*

 [ISSN 2581-5369]

Consumer Protection Act, 2019, the Competition Act, 2002, and the Digital Personal Data Protection Act, 2023. While these laws provide a robust foundation, they were not designed specifically for digital markets and face several limitations. The Consumer Protection Act's penalty provisions are modest compared to platform revenues, potentially making violations a cost of doing business. The Competition Act's ex-post enforcement approach struggles with fast-moving digital markets where harm may become irreversible before remedies are implemented. The Digital Personal Data Protection Act's consent-based framework may be inadequate for addressing structural power imbalances. Regulatory fragmentation across multiple authorities creates coordination challenges, definitional inconsistencies, and enforcement gaps.

Enforcement challenges are particularly acute regarding multinational corporations, which employ complex corporate structures, strategic litigation tactics, and resource advantages to resist regulatory oversight. Penalties imposed to date have been criticized as insufficient to deter violations, and jurisdictional challenges regarding foreign entities and cross-border data flows complicate enforcement. The multinational corporation accountability gap represents a critical weakness in India's regulatory architecture.

Comparative analysis of regulatory approaches in the European Union, United Kingdom, and United States yields important lessons for India. The EU's Digital Markets Act demonstrates that ex-ante regulation with clear designation criteria and comprehensive obligations can address structural issues more effectively than ex-post enforcement alone. The UK's pro-competition regime shows the value of tailored interventions addressing market-specific concerns. The US experience highlights both the potential and limitations of relying on traditional antitrust enforcement. All three jurisdictions emphasize the need for substantial penalties linked to global turnover, strong regulatory capacity, and international cooperation.

B. Policy Implications and Future Outlook

The findings of this article support the case for enacting digital markets-specific legislation in India, as recommended by the Committee on Digital Competition Law. Such legislation should establish an ex-ante regulatory framework for Systemically Significant Digital Enterprises, with clear designation criteria, comprehensive obligations addressing multiple dimensions of platform conduct, and strong enforcement mechanisms including substantial penalties and structural remedies. The legislation should be complemented by amendments to the Consumer Protection Act and Competition Act to enhance penalties, strengthen enforcement powers, and address digital market-specific practices.

 [ISSN 2581-5369]

Equally important is strengthening institutional capacity and coordination. The Competition Commission of India, Central Consumer Protection Authority, and Data Protection Board require substantially increased resources, technical expertise, and investigative powers to effectively regulate digital markets. Formal coordination mechanisms including joint guidelines, information sharing protocols, and coordinated enforcement actions are essential to address practices that implicate multiple legal domains. International cooperation through bilateral and multilateral agreements will be critical for enforcing against multinational corporations and addressing cross-border challenges.

Consumer empowerment through digital literacy programs, transparency tools, accessible complaint mechanisms, and support for consumer organizations should complement regulatory enforcement. Informed and empowered consumers can make better choices, identify unfair practices, and hold platforms accountable, creating market-based incentives for fair dealing.

The future trajectory of India's digital economy will depend significantly on the regulatory choices made in the coming years. Without effective regulation, market concentration is likely to increase, unfair trade practices will proliferate, and the benefits of digitalization will accrue disproportionately to dominant platforms at the expense of consumers, small businesses, and innovation. With appropriate regulation, India can create a digital marketplace that is fair, transparent, contestable, and conducive to innovation and inclusive growth.

C. Limitations and Future Research Directions

This article has several limitations that suggest directions for future research. First, while the analysis draws on secondary data on the prevalence and impact of specific unfair trade practices in Indian digital markets remains limited. Future research should conduct systematic surveys of consumer experiences, analyse platform data (where accessible), and quantify the economic and social harms of unfair practices.

Second, this article focuses primarily on legal and regulatory analysis, with limited attention to technical dimensions of algorithmic systems, platform architectures, and data processing practices. Interdisciplinary research combining legal analysis with computer science, economics, and behavioural science would provide deeper insights into how unfair practices operate and how they can be detected and remedied.

Third, the article examines enforcement challenges but does not provide detailed analysis of specific cases and their outcomes. Case study research examining how regulatory authorities have addressed particular unfair practices, what obstacles they encountered, and what lessons can be learned would inform more effective enforcement strategies.

 [ISSN 2581-5369]

Fourth, the comparative analysis focuses on the European Union, United Kingdom, and United States, with limited attention to regulatory approaches in other emerging digital economies. Comparative research examining approaches in countries like Brazil, South Korea, Japan, and Australia would provide additional insights relevant to India's context.

Fifth, the article proposes policy recommendations but does not assess their potential economic impacts, implementation challenges, or political feasibility. Future research should conduct detailed impact assessments of proposed reforms, including effects on innovation, investment, consumer welfare, and market structure.

Finally, digital markets are rapidly evolving, with emerging technologies like artificial intelligence, blockchain, and the metaverse creating new forms of market intermediation and new potential for unfair practices. Future research should examine how regulatory frameworks can adapt to these technological developments while maintaining core principles of fairness, transparency, and contestability.

The regulation of unfair trade practices in India's digital economy is at a critical juncture. The legal and institutional foundations have been established, but significant reforms are necessary to address the unique challenges of digital markets and ensure that the benefits of digitalization are broadly shared. This article has sought to contribute to the ongoing policy debate by providing comprehensive analysis of the problem, examining the current regulatory framework, learning from global experiences, and proposing concrete reforms. The ultimate goal is a digital marketplace that serves the interests of all participants consumers, businesses, workers, and society rather than entrenching the power of a few dominant platforms.

*****

 [ISSN 2581-5369]

IX. REFERENCES

1. Advertising Standards Council of India, Guidelines for Influencer Advertising in Digital Media (2021).
2. Ayilyath, "Consumer Protection in E-Commerce Transactions in India – Need for Reforms" (2020) Social Science Research Network, DOI: 10.2139/SSRN.3571069.
3. Bhat, "Data Sharing for Contestability in Data-Driven Digital Markets: An Analysis" (2023) 4 *Competition Commission of India Journal on Competition Law and Policy* 113, DOI: 10.54425/ccijoclp.v4.113.
4. Bureau of Indian Standards, *Standards for Environmental Claims* (2023).
5. Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023 (2023).
6. Chauhan et al., "Darker Patterns? AI-generated Persuasion and the Regulatory Void in Indian Law" (2024) *Journal of Development Policy and Practice*, DOI: 10.1177/24551333241275752.
7. Chugh et al., "Unpacking dark patterns: Understanding dark patterns and their implications for consumer protection in the digital economy" (2024).
8. *Competition Act, 2002* (Act No. 12 of 2003).
9. Competition Commission of India Journal on Competition Law and Policy (2020).
10. Consumer Protection Act, 2019 (Act No. 35 of 2019).
11. Consumer Protection (E-Commerce) Rules, 2020.
12. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
13. European Commission, Designation Decisions under the Digital Markets Act (2024).
14. Gupta, "Artificial intelligence and competition law in India: A legal response to algorithmic market collusions" (2025) 15(3) *European Economics Letters*, DOI: 10.52783/eel.v15i3.3450.
15. Jain et al., "Regulating Competition in Digital Markets" (2024) *ICRIER Prosus Centre for Internet and Digital Economy*.
16. Kumar, "Consumer Protection in the Digital Era: A Critical Analysis of Legal Safeguards against Online Shopping Fraud" (2025) 5(1) *Research Review Journal of Social Science*, DOI: 10.31305/rrjss.2025.v05.n01.026.

17. Kumar et al., "Fair and Competitive E-marketplaces (F.A.C.E.) | The Business Users' Narrative" (2021) *Working Paper*.

18. Larionova et al., "India. Developing Regulation of Technological Platforms for Digital Economy Growth" (2024).

19. Legal Metrology (Packaged Commodities) Rules, 2011.

20. Mahaur, "E-Commerce & Consumer Rights: Navigating Protection in India's Digital Marketplace" (2024).

21. Ministry of Corporate Affairs, Report of the Committee on Digital Competition Law (2024).

22. Padmavathy Nehru, "DIGITAL ECONOMY & COMPETITION LAW: A CONUNDRUM" (2022) *Indian Journal of Legal Review*.

23. Pathak, "Legal and Commercial Dynamics of E-Consumer Protection: Navigating Challenges in India's Digital Economy" (2024) 6(5) *International Journal For Multidisciplinary Research*, DOI: 10.36948/ijfmr.2024.v06i05.28398.

24. Raj et al., "Safeguarding the Digital Consumer: A Comparative Legal and Psychological Analysis of Dark Patterns in E-Commerce" (2024).

25. Reddy, "Promotion and Regulation of E-Commerce in India" (2022) *Parliament of India, Rajya Sabha*.

26. Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).

27. Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market **For** Digital Services (Digital Services Act).

28. Sakle et al., "The Interaction between Competition Law & Digital and E-commerce Markets in India" (2020) 16 *Indian Journal of Law and Technology*, DOI: 10.55496/kvug7838.

29. Samritha et al., "A Study on Regulation of E-Commerce in India: Issues and Challenges" (2025), DOI: 10.5281/zenodo.17035441.

30. Sharma, "Dark patterns in a bright world: an analysis of the Indian consumer legal architecture" (2024).

31. Singh, "Amazon's Competition Investigation in India: A Case for Expansion of Investigation and Grant of Interim Relief" (2020) *Indian Journal of Law and*

Technology, DOI: 10.55496/pkvm6266.

32. Singh et al., "Platform-Based Internationalization of Smaller Firms: The Role of Government Policy" (2022) *Management International Review*, DOI: 10.1007/s11575-022-00492-z.

33. Singh et al., "Prioritizing dark patterns in the e-commerce industry–an empirical investigation using analytic hierarchy process" (2024).

34. Tamilmani et al., "Impact of Dark Patterns in E-Commerce on Consumer Rights" (2024).

35. Tewari, "A Critical Evaluation of India's Proposed Digital Competition Act" (2024) 5 *Competition Commission of India Journal on Competition Law and Policy* 197, DOI: 10.54425/ccijoclp.v5.197.

36. UK Competition and Markets Authority, *Digital Markets Unit* (2021).

37. UK Digital Markets, Competition and Consumers Act 2024.

38. U.S. Federal Trade Commission and Department of Justice, *Antitrust Enforcement in Digital Markets* (2024).

39. Yadav, "Strengthening consumer consent in e-commerce: Legal and policy reforms to address dark patterns and AI-driven challenges" (2024).

*****

 [ISSN 2581-5369]