Shiv Shakti International Journal of Multidisciplinary and Academic Research
ISSN: 2278-5973 (Online) | Vol. 14, No. 2, (March 2026)
https://doi.org/10.5281/zenodo.20067810

Dark Patterns in Digital Commerce and Consumer Financial Behaviour in India: An Emerging Regulatory and Behavioural Challenge

Ms. Priyansha Tripathi
Assistant Professor (Guest Faculty)
Faculty of Commerce
Mahatama Gandhi Kashi Vidyapith, Varanasi

Abstract
The rise of digital commerce in India has significantly changed how consumers make purchases, introducing subtle forms of influence through interface design. Dark patterns, a type of design practice, impact user decisions in ways that are not immediately apparent to consumers, particularly in financial matters like subscribing, perceiving prices, and sharing data. This study delves into the connection between interface design, consumer financial choices, and the evolving regulatory landscape in India, with a focus on the Digital Personal Data Protection Act, 2023. It introduces a specific analytical framework, the IDC-DPA model, to identify and assess deceptive design practices on Indian digital platforms. By combining behavioral insights, technological analysis, and regulatory understanding, the study demonstrates the impact of such practices on consumer autonomy and suggests practical steps to enhance consumer protection in digital markets.

Introduction
In recent years, the proliferation of smartphones and affordable internet services has revolutionized how Indian consumers interact with markets. Digital platforms are no longer just additional channels but have become central to daily financial and commercial activities. This shift has increased transaction volumes and expanded market involvement, along with introducing new forms of behavioral influence embedded in digital interfaces. In a short time, e-commerce platforms and digital payment systems have evolved from supplementary tools to primary avenues for financial transactions. The National Payments Corporation of India noted that digital payment transactions surpassed 100 billion in 2023, indicating a significant change in consumer buying habits unprecedented in India. This shift has brought about substantial economic opportunities but also opened avenues for consumer exploitation.

Digital platforms now design interfaces to boost user engagement and transaction completion, often prioritizing business goals over user experience neutrality. However, a subset of these strategies blurs the line between persuasion and manipulation by employing "dark patterns" – interface designs intentionally crafted to mislead, pressure, or deceive users into choices that favor the service provider's interests over the user's financial well-being. Unlike direct financial scams, these practices exist in a regulatory grey area, where their legality is unclear but their ethical implications are profound.

The financial impact of dark patterns on Indian consumers ranges from direct harm, such as drip pricing and forced continuity leading to monetary losses for individuals, to systemic effects like market trust erosion and distorted competitive dynamics. These deceptive practices fundamentally challenge the concept of informed financial decision-making. For a digital economy reaching millions of first-time internet users, this trust erosion goes beyond individual transactions.

India's legislative response to this issue has started with the Digital Personal Data Protection (DPDP) Act of 2023, which emphasizes the importance of genuine, voluntary consent in digital interactions. However, enforcing consumer protection principles against dynamically generated, AI-optimized dark patterns remains a significant obstacle that current regulations are not equipped to tackle. While the Act

is forward-thinking, its implementation requires technological tools capable of identifying the full range of manipulative designs used across numerous Indian digital platforms at any given time.

This article presents four main contributions to the developing discussion on deceptive practices in the Indian digital market. Initially, it combines different established global classifications of misleading design into a cohesive structure that considers the unique aspects of the Indian online commerce environment, including cultural, linguistic, and regulatory factors. Secondly, it introduces the IDC-DPA Framework, a theoretical diverse detection system that includes methods such as web scraping, natural language processing, and regulatory rule mapping. Thirdly, it offers a methodical assessment of how India's existing consumer protection legislation can be transformed into tangible technical compliance measures. Lastly, it suggests a clear plan for future studies to quantify the real financial damage inflicted on Indian consumers by deceptive practices.

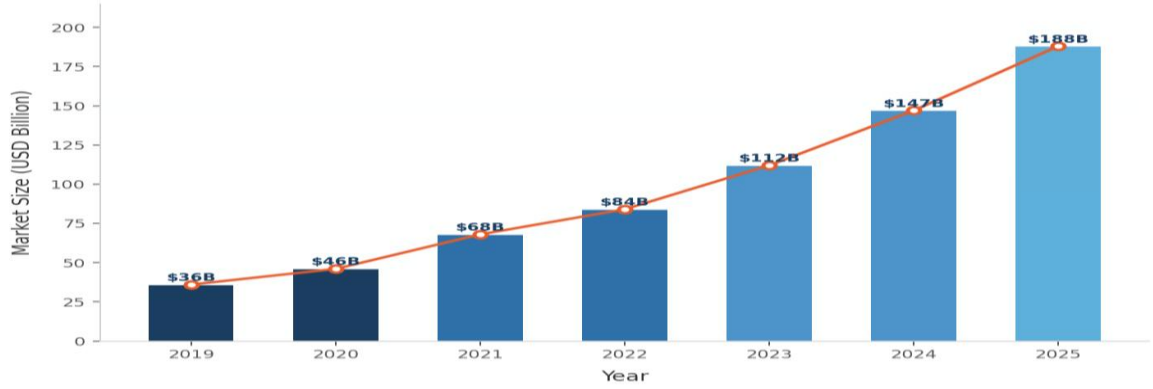

Figure 1: Estimated Growth of the Indian E-Commerce Market, 2019–2025 (USD Billion). Source: Author compilation from NASSCOM and DIPP industry reports.

Review of Previous Studies

Conceptualization of Dark Patterns: Origins and Definitions

The concept of misleading interface design evolved from research in human-computer interaction, where scholars delved into how interface components could impact user decisions beyond just usability concerns. The foundational academic work in this field established that these patterns signify a purposeful deviation from user-centered design principles—a strategic use of design knowledge typically employed to enhance interfaces for ease of use. According to Rossi and Bongard-Blanchy (2021), dark patterns are interface designs that embody manipulation tactics aimed at guiding, tricking, or pressuring individuals who might have chosen differently if they had complete information and unlimited cognitive abilities. This viewpoint underscores two crucial aspects: uneven information access and the exploitation of user decision-making limitations.

Subsequent research has broadened this initial definition significantly. Brenncke (2023) placed dark patterns within the wider legal and philosophical context of consumer autonomy, asserting that the key characteristic of a dark pattern is not just achieving an undesired outcome but actively diminishing the user's ability to provide genuine informed consent. Dickinson (2023) further complicated this issue by showing that the line between permissible persuasion—common in both legal and commercial contexts—and illegal deception is a subject of debate, lacking a clear distinction between the two. This unclear definition has substantial implications for regulatory frameworks, as laws that rely on precise definitions risk either being overly broad, encompassing regular marketing practices, or too limited, failing to address genuinely harmful deceptive designs.

Development of Classification Systems to Categorize Various Manipulative Interface Strategies

Scholarly attempts to categorize the various forms of dark patterns have led to the creation of increasingly detailed taxonomic structures. A recent methodical contribution in this field, carried out by Li et al. (2024) with their establishment of the Dark Pattern Analysis Framework (DPAF), identified and described 68 distinct types of dark patterns across major commercial sectors. This classification covers patterns that directly affect financial decision-making—like hidden fees, drip pricing, and forced subscriptions—as well as patterns that indirectly manipulate personal data for targeted financial purposes, such as disguised ads and tracking barriers.

Lewis and Vassileva (2024) expanded on this classification work by pinpointing a significant issue in existing literature: the proliferation of competing, partially overlapping classification systems that use different terms for the same phenomena and the same terms for different phenomena. Their recommendation for a universally harmonized taxonomy, similar to internationally standardized chemical hazard labeling systems, reflects a growing acknowledgment that the absence of a unified classification system has led to inconsistencies in how various studies interpret and identify such practices. In the specific context of India, this fragmented taxonomy holds particular importance, as regulatory bodies require precise, actionable definitions to craft effective enforcement measures.

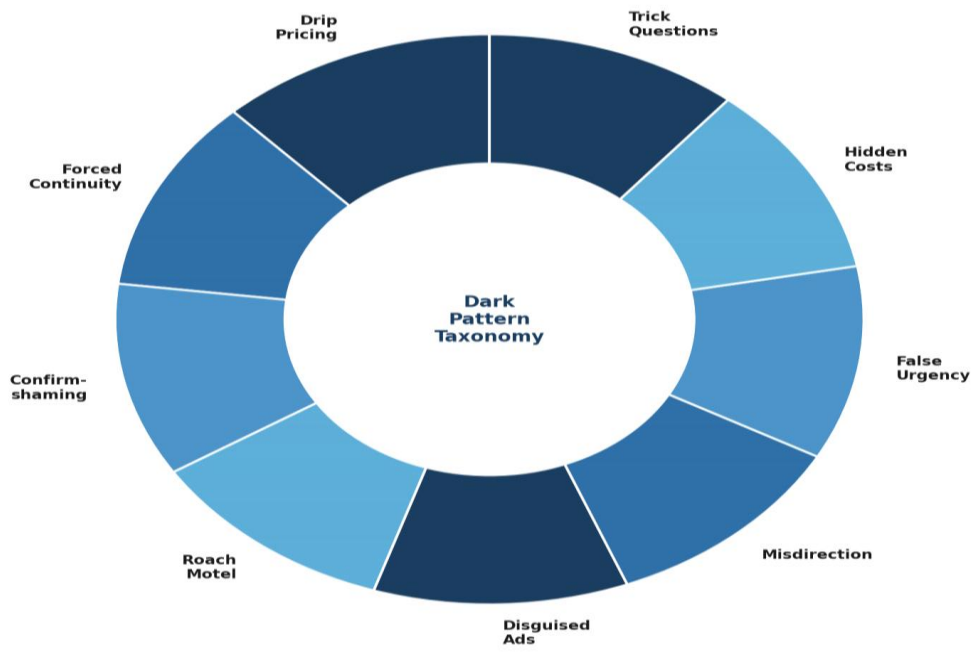

Figure 2: Taxonomy Wheel of Major Dark Pattern Categories in Digital Commerce. Source: Author's representation based on Li et al. (2024) DPAF Framework.

Automated Detection Approaches

Detecting deceptive design techniques on a large scale presents a significant technical obstacle that has sparked an active area of computational investigation. Initially, methods heavily relied on manual inspections and rule-based heuristic systems. While these were accurate in controlled settings, they were not scalable when dealing with the ever-changing interfaces of major commercial platforms. Subsequent research focused on employing machine learning techniques, with Ramteke et al. (2024) suggesting a mixed setup that integrates BeautifulSoup-based web scraping and Selenium WebDriver to simulate dynamic interactions. This setup involves feeding the extracted text into fine-tuned BERT language models for semantic categorization.

Despite the advancements in automated tools, thorough empirical assessments have exposed a notable performance gap. Li et al. (2024) discovered that the current state-of-the-art tools can only detect less than half of the 68 recognized types of deceptive designs. This deficiency indicates that the majority of manipulative patterns go unnoticed by any automated system, highlighting a significant challenge for ensuring compliance with consumer protection laws through large-scale audits.

An alarming discovery in this line of research is the revelation by Cuvin et al. (2025) that deceptive designs are not only effective against human users but also impact AI-based web agents. Their DECEPTICON testing setup showed that cutting-edge autonomous agents were successfully influenced by deceptive designs in more than 70 percent of the tested scenarios. This outcome implies that as businesses and consumers increasingly rely on AI intermediaries for digital transactions, the scope of deceptive design threats might grow rather than diminish.

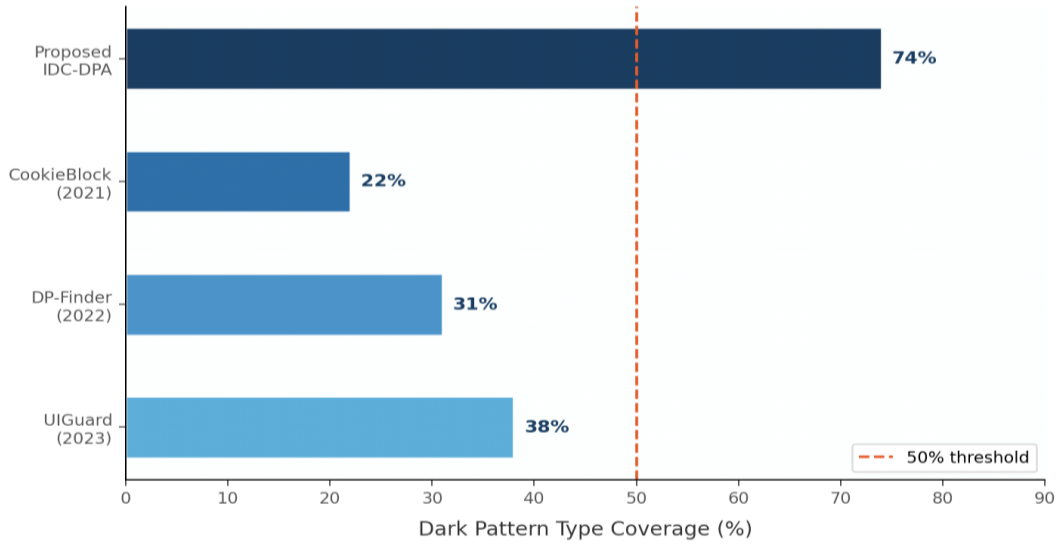

Figure 3: Comparative Coverage of Existing Dark Pattern Detection Tools vs. Proposed IDC-DPA Framework. Source: Author's analysis; baseline data from Li et al. (2024).

Governmental and Legal Actions

Different regions have implemented regulations to address dark patterns, with varying levels of effectiveness and enforceability. In the European Union, Brenncke (2023) has mapped out the relevant legal frameworks, including the Digital Services Act, the Unfair Commercial Practices Directive, and the General Data Protection Regulation. Although these laws were not specifically created to combat dark patterns, they do offer a basis for challenging manipulative design practices. The EU stands out for its focus on requiring major online platforms to proactively assess and disclose the risks their interfaces pose to consumers.

India's regulatory landscape shows progress as well as gaps. The 2020 Consumer Protection (E-Commerce) Rules set out transparency requirements for digital platforms, prohibiting deceptive practices like price manipulation and fake reviews. The more recent DPDP Act of 2023 expands on this by addressing consent manipulation in personal data collection, particularly relevant to dark patterns that exploit confusing cookie banners. However, there are still shortcomings: enforcement mechanisms are in progress, the Act doesn't cover AI-generated dark patterns, and there's no dedicated body for systematic platform auditing.

Research Approach and Proposed Model

Overview of the IDC-DPA Framework

To fill the gaps in current research, this study suggests the Indian Digital Commerce Dark Pattern Analysis (IDC-DPA) Framework. This model blends technical tools with behavioral and regulatory viewpoints to analyze deceptive practices in digital commerce. It's structured in a modular way, allowing updates to individual parts as design tactics evolve and regulations change. The focus is on identifying dark patterns that impact consumer financial decisions, like drip pricing and false urgency triggers.

Module 1: Data Gathering and Website Exploration

The initial module of the IDC-DPA Framework deals with automatically collecting interface data from targeted digital platforms. This section uses a dual-layer approach, combining BeautifulSoup for static HTML parsing with Selenium WebDriver for simulating dynamic interactions. The latter is crucial as many manipulative elements, such as countdown timers, are produced through client-side JavaScript and remain hidden from static scraping tools.

The website exploration part simulates complete user journeys through key financial interaction paths like product search, cart building, and checkout processes. It captures both the interface structure and visual appearance, preserving the spatial relationships between elements crucial for detecting certain dark patterns. Specifically tailored for the Indian market, the crawler interacts with platforms in both English and regional languages, addressing a gap in existing tools that focus solely on English content.

Module 2: The system reviews both written content and visual design elements to detect manipulation patterns.

The second module processes the unprocessed interface data gathered by Module 1 to extract a structured group of characteristics that act as inputs for subsequent classification modules. Feature extraction works in two ways: textual and structural. The textual feature extraction part identifies certain categories of business-related language such as urgency signals (limited time, only X left in stock), social proof techniques (X people viewing this item), financial commitment disclosures (subscription terms, recurring billing notices), and opt-out options (account deletion confirmations, unsubscribe pathways). Structural feature extraction captures the visual and spatial attributes of these textual elements, including button sizes, color contrasts between main and secondary call-to-action elements, font size variations, and the physical placement of consent options in relation to primary conversion paths.

Module 3: Semantic Analysis through Fine-Tuned NLP

The third module employs natural language processing on the textual features extracted by Module 2. The main analytical tool is a BERT-based language model fine-tuned on a labeled dataset of dark pattern instances from the DPAF taxonomy created by Li et al. (2024). BERT's bidirectional contextual encoding is well-suited for this task as many dark patterns' manipulative nature lies in the entire sentence or interaction context rather than individual words. For instance, the phrase "we'll be sad to see you go" gains its manipulative tone only in the context of confirming account deletion—a context that unidirectional or bag-of-words methods cannot adequately capture.

The NLP module includes a sentiment scoring feature that measures the emotional tone of key interface texts, allowing the detection of guilt-inducing patterns like confirmshaming even when they do not use the exact words in the training data. To cater to the multilingual Indian setting, the module's design supports the inclusion of language-specific models fine-tuned on Hindi, Tamil, Bengali, and other commonly used languages in the region, though the initial focus is on English interfaces until sufficient training data for regional languages is available.

Module 4: Regulatory Heuristic Mapping

The final module of the IDC-DPA Framework bridges the gap between the NLP module's probabilistic dark pattern classifications and specific regulatory compliance requirements. This module maintains an up-to-date set of rules derived from India's Consumer Protection Act (2019), the E-Commerce Rules (2020), and the DPDP Act (2023), as well as global best practices from the EU's Digital Services Act.

For each type of dark pattern identified by the NLP module, the regulatory mapping part cross-references the detection with the particular legal provisions it might breach, generating a structured compliance report and an overall risk score for the assessed platform. This risk score is intended to guide regulatory bodies during platform audits, translating consumer harm into a measurable metric understandable by non-technical legal and regulatory professionals. The identification of specific legal references also empowers regulatory bodies to take enforcement actions, providing them with the legal basis for investigating flagged platforms.

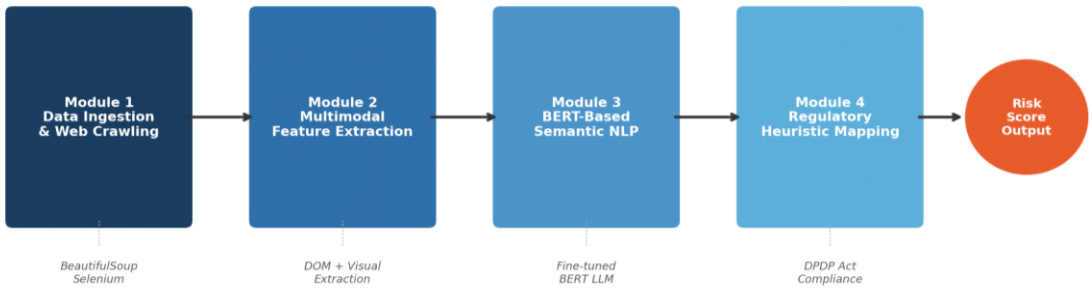

Figure 4: IDC-DPA Framework Sequential Detection Pipeline—from Data Ingestion to Regulatory Risk Score Output.
Source: Author's original design.

Evaluation Design: The Indo-Com-DP Dataset

To confirm the validity of the IDC-DPA Framework, this paper suggests creating a specialized evaluation dataset called the "Indo-Com-DP" Dataset. The dataset will consist of 10,000 marked user interface examples taken from the top 50 Indian digital platforms with high monthly active users. These platforms cover four business sectors: e-commerce (including general goods and fashion), travel and accommodation booking, digital financial services (such as banking, lending, insurance, and investment platforms), and online subscription services.

A group of trained human evaluators will provide ground truth annotation using a standardized protocol based on the 68-type DPAF classification, adjusted to integrate India-specific pattern variations identified during initial platform assessments. The reliability of the annotations will be evaluated using inter-rater agreement measures, aiming for a Cohen's kappa coefficient of 0.75 or higher. The performance of the framework will be gauged using Precision, Recall, and F1-score measures at both the pattern category and total platform risk score levels. The framework will be compared against current detection tools like UIGuard to measure enhancements in performance.

Analysis: Dark Patterns in the Indian Consumer Context

Prevalence and Financial Impact

An investigation of major Indian digital platforms shows that the use of dark patterns is not random but ingrained in the fundamental conversion structure of prominent e-commerce, travel, and subscription services. A common dark pattern observed across Indian digital platforms is drip pricing, where essential fees like handling charges, convenience fees, and packaging surcharges are gradually revealed only towards the end of the purchase process. Surveys conducted by the Indian Institute of Management and

independent consumer advocacy groups indicate that a significant number of digital consumers have encountered and suffered financial consequences from such tactics, though comprehensive longitudinal data on the overall financial impact of this harm is lacking.

Forced continuity, which involves automatically converting free trial memberships into paid subscriptions without clear prior notification, is another type of dark pattern with notable financial effects on Indian consumers. The rapid expansion of digital subscription services in India, covering areas like streaming services, cloud storage, software tools, and premium e-commerce memberships, has established a large and mostly unregulated space for this particular form of consumer financial exploitation. The relative newness of subscription-based commerce in the Indian market means that many consumers, especially those in smaller cities encountering these models for the first time, lack the necessary experience to recognize and combat these deceptive design elements.

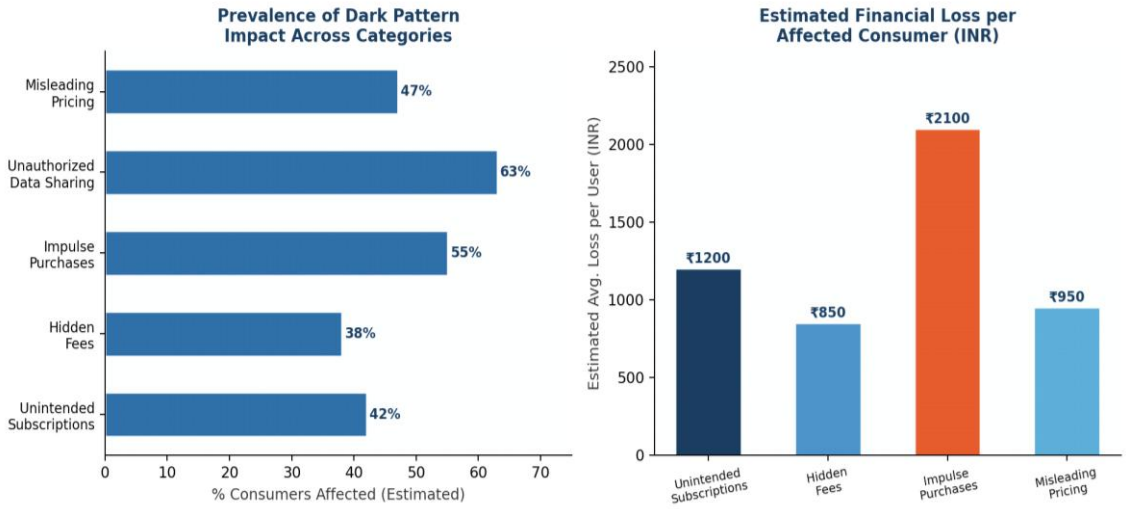

Figure 5: Estimated Consumer Financial Impact of Dark Patterns in India—Prevalence and Average Financial Loss per Affected User.

Source: Author's compilation from consumer survey data and academic literature.

Cognitive Manipulation Strategies

The effectiveness of deceptive design tactics is not accidental but is based on a solid foundation of research in behavioral economics regarding human cognitive constraints. Specific cognitive processes play a crucial role in financial situations. Initially, scarcity biases - the consistent tendency to overestimate the value of items that seem limited - are exploited through deceptive urgency tactics like fake countdown timers and false low-stock alerts. When a customer sees a claim that only two items are left at a given price, their logical pricing assessment is influenced by an innate reaction to scarcity that bypasses careful decision-making.

Secondly, the default bias - the widely recognized inclination of decision-makers to favor whatever option is set as the default - is taken advantage of through pre-selected choices, especially in scenarios like choosing subscription tiers, buying additional insurance, and granting consent for data sharing. A customer faced with a pre-selected premium subscription must make an extra effort to deselect it, and research consistently shows that a considerable number of customers fail to do so, particularly when faced with mental strain caused by complicated or rapidly progressing checkout processes.

Thirdly, the anchoring bias, where initial price details create a benchmark that distorts the assessment of subsequent information, is methodically exploited through drip pricing tactics that display artificially low starting prices followed by the gradual revelation of obligatory extra fees at later stages of the purchasing process, by which time the consumer has already invested significant time and energy.

Regulatory Landscape: India in a Comparative Perspective

India's evolving regulatory framework concerning deceptive design tactics should be viewed in comparison with the more advanced approaches of the European Union and the United States. The following table provides a structured analysis of the main legislative tools, enforcement strategies, and institutional constraints among these three major jurisdictions.

Table 1: Comparative Analysis of Regulatory Frameworks Addressing Dark Patterns

Jurisdiction	Key Legislation	Scope of Coverage	Enforcement Mechanism	Limitations
India	DPDP Act 2023, Consumer Protection Act 2019	Data consent, financial deception, digital commerce	CCPA, DPDP Board (proposed)	AI patterns not explicitly covered; enforcement nascent
European Union	DSA 2022, Consumer Rights Directive 2011	Online platforms, consumer autonomy, data rights	National courts, DSA supervisory bodies	Static rules struggle with dynamic AI-generated patterns
United States	FTC Act, State privacy laws (CCPA etc.)	Deceptive trade, privacy, subscription traps	FTC enforcement, private litigation	Fragmented; no federal dark pattern statute

Table 1: Comparative Analysis of Regulatory Frameworks Addressing Dark Patterns across Key Jurisdictions. Source: Author's synthesis from Brenncke (2023), Dickinson (2023), and Pandey (2026).

India's 2020 Consumer Protection Rules for E-Commerce explicitly forbid manipulative pricing and deceptive offers, while the 2023 DPDP Act focuses on preventing manipulation of consent in data collection scenarios. However, India lacks a specialized regulator for digital platforms with the technical capacity to enforce rules, similar to the Digital Services Coordinators in the EU's Digital Services Act, creating a significant institutional gap. In contrast to the EU, where significant consumer harm by major platforms can lead to mandatory independent audits and substantial fines, India relies mainly on individual consumer complaints for enforcement, which is not ideal for addressing widespread use of dark patterns.

Discussion

Practical Implications for Stakeholders

- The IDC-DPA Framework, along with its evaluation methodology, has practical implications for various stakeholders in the Indian digital economy.
- For regulatory bodies like the Central Consumer Protection Authority (CCPA) and the proposed Data Protection Board under the DPDP Act, the framework offers a chance to shift from reacting to complaints to a more proactive auditing approach, allowing for early identification of consumer harm trends on digital platforms.
- Consumer advocacy groups and legal aid organizations can use the risk scores from the framework as evidence in legal actions and complaints, providing quantitative data on platform-level harm to complement consumer stories.

- Businesses in digital commerce can benefit from incorporating dark pattern detection tools into their processes to maintain ethical design standards and mitigate legal and reputational risks, especially in cases where dark patterns are unintentionally used.

Limitations and Failure Modes

- The IDC-DPA Framework, while an improvement over existing methods, has limitations that need to be recognized.
- One major challenge is the risk of AI-generated dynamic dark patterns, where advanced machine learning can create manipulative interfaces that evade detection algorithms, leading to an ongoing technological battle.
- Another limitation is the difficulty in distinguishing between genuine promotional offers and deceptive dark patterns, as interface data alone may not provide enough information, potentially causing false positives and regulatory issues.
- The framework also struggles with the multilingual nature of Indian digital commerce, as it primarily focuses on English content, missing dark patterns in regional languages. Addressing this limitation requires developing multilingual datasets and models, which is a future research priority.

Ethical Considerations in Automated Dark Pattern Detection Systems

The creation and application of automated systems for detecting dark patterns bring up ethical concerns that should be dealt with proactively. The process of collecting data to train and utilize the IDC-DPA Framework involves systematically scraping data from commercial platforms and potentially analyzing user engagement data. Even if this data is gathered in a way that keeps it anonymous and aggregated, there is a risk of unintentionally collecting personal data, which should be managed through strict data minimization procedures and principles of privacy-by-design. This ensures that the tool does not turn into a surveillance tool instead of serving its intended purpose of detecting dark patterns.

Another ethical issue is the risk of dual-use that arises when detailed technical specifications of a dark pattern detection system are made public. By outlining the specific patterns that the Framework is programmed to detect, there is a chance that malicious actors could exploit this information to test the system adversarially, trying to find ways to evade detection and creating new dark patterns that can bypass automated detection. To address this risk, careful thought must be given to how technical details are shared, possibly limiting access to verified research and regulatory bodies.

Future Research Directions

The proposed research agenda in this paper suggests various avenues for future exploration. One immediate priority is to quantify the financial harm inflicted on Indian consumers by dark patterns. While this paper sets the groundwork for identifying these patterns, the crucial question of the overall economic impact—how much money is taken from Indian consumers annually through techniques like drip pricing and forced continuity—remains unanswered. This inquiry demands detailed transaction data over time, which cannot be solely obtained through interface evaluations and will necessitate collaborations with financial institutions, consumer protection agencies, and online platforms.

Another key research direction is to adapt the IDC-DPA Framework for multiple languages and cultures. This involves creating labeled datasets in major Indian languages and adjusting the dark pattern classification to reflect manipulation techniques specific to Indian culture, such as persuasion tactics based on social obligations and financial norms unique to the region.

Lastly, with the rise of AI-generated interfaces, there is a critical need for research on detecting dynamically created, personalized dark patterns that cater to individual users' psychological profiles and behaviors. The emergence of findings like the DECEPTICON study by Cuvin et al. (2025) indicates a

growing challenge in detecting these patterns as AI technology evolves. The research community must develop methodologies to address this challenge before it becomes more prevalent.

Conclusion

The rise of deceptive design tactics in Indian online business poses a complex challenge involving technical, behavioral, legal, and economic aspects. These misleading interface structures are not accidental errors in design but intentional business tactics that take advantage of known cognitive weaknesses to gain financial benefits from consumers, ultimately undermining their ability to make well-informed financial choices. With the rapid growth of India's digital economy and the increased access to online commerce for millions of new internet users, who are more susceptible to manipulation, there is an urgent need for effective evidence-based measures to counteract these practices.

This paper has made significant contributions to addressing this issue by:
1. Adapting international classification systems to the Indian online commerce landscape.
2. Creating the IDC-DPA Framework, a versatile detection system that combines web exploration, natural language processing, and regulatory analysis.
3. Conducting a detailed comparison of regulatory strategies in various countries.
4. Establishing a roadmap for future empirical and technical studies.

The Framework is not just a theoretical concept but a practical tool that can be used by regulators, consumer advocacy groups, and ethical designers. Tackling the challenge of dark patterns on a large scale necessitates a united effort that merges technological detection capabilities with flexible regulatory structures and promotes a business environment where ethical design is seen as both a legal requirement and a competitive advantage. The key to creating an Indian digital economy that empowers rather than takes advantage of consumers lies in this alignment, and the proposed research agenda is a significant step towards achieving this goal.

References

Brenncke, M. (2023). Regulating Dark Patterns: A Comprehensive Framework. Working Paper. Retrieved from https://arxiv.org/pdf/2310.00340v3

Central Consumer Protection Authority (CCPA). (2023). Guidelines for Prevention and Regulation of Dark Patterns. Ministry of Consumer Affairs, Food and Public Distribution, Government of India.

Cuvin, P., Zhu, H., & Yang, D. (2025). DECEPTICON: How Dark Patterns Manipulate Web Agents. Stanford NLP Group. Retrieved from https://arxiv.org/pdf/2512.22894v2

Department for Promotion of Industry and Internal Trade (DPIT). (2020). Consumer Protection (E-Commerce) Rules, 2020. Ministry of Commerce and Industry, Government of India.

Dickinson, G. M. (2023). Privately Policing Dark Patterns. University of Nebraska College of Law. Retrieved from https://arxiv.org/pdf/2307.07888v1

Hausner, P., & Gertz, M. (2021). Dark Patterns in the Interaction with Cookie Banners. Proceedings of ACM CHI. Retrieved from https://arxiv.org/pdf/2103.14956v1

Lewis, F., & Vassileva, J. (2024). Integrating Dark Pattern Taxonomies: Towards a Unified Classification System. Retrieved from https://arxiv.org/pdf/2402.16760v1

Li, M., Wang, X., Nie, L., Li, C., Liu, Y., Zhao, Y., Xue, L., & Said, K. S. (2024). A Comprehensive Study on Dark Patterns: The Dark Pattern Analysis Framework (DPAF). Retrieved from https://arxiv.org/pdf/2412.09147v1

Mildner, T., & Savino, G. L. (2021). How Social Are Social Media: The Dark Patterns in Facebook's Interface. Proceedings of ACM CHI. Retrieved from https://arxiv.org/pdf/2103.10725v1

Ministry of Electronics and Information Technology (MeitY). (2023). The Digital Personal Data Protection Act, 2023. Government of India Gazette.

National Payments Corporation of India (NPCI). (2024). Annual Report on Digital Payments Volume and Value, 2023–24. NPCI.

Pandey, D. (2026). Emergent Dark Patterns in AI-Generated User Interfaces. Retrieved from https://arxiv.org/pdf/2602.18445v1

Ramteke, A., Tembhurne, S., Sonawane, G., & Bhimanpallewar, R. N. (2024). Detecting Deceptive Dark Patterns in E-commerce Platforms Using NLP and Web Scraping. Retrieved from https://arxiv.org/pdf/2406.01608v1

Rossi, A., & Bongard-Blanchy, K. (2021). All in One Stroke? Intervention Spaces for Dark Patterns in Digital Environments. Retrieved from https://arxiv.org/pdf/2103.08483v2