Advances in Consumer Research
ISSN (Print): 0098-9258
ISSN(Online): 3079-1766

Vol. 2, Issue 4 (2025) https://acr-journal.com/

Safeguarding the Digital Consumer: A Comparative Legal and Psychological Analysis of Dark Patterns in E-Commerce

Prithivi Raj[1], Sobhagya Sundar Nanda[2], Chinmayee Das[3], Yogendra Singh[4], Swagat Dash[5], Ashmika Agrawal[6]

[1]Assistant Professor of Law, Birla Global University, India
[2]Assistant Professor of Law, Birla Global University, India
[3]Assistant Professor of Law, Siksha O Anusandhan (Deemed to be University), India
[4]Assistant Professor of Law, Birla Global University, India
[5]Assistant Professor of Law, Birla Global University, India
[6]Assistant Professor of Law, Amity University, India

Cite this paper as: Prithivi Raj, Sobhagya Sundar Nanda, Chinmayee Das, Yogendra Singh, Swagat Dash, Ashmika Agrawal, (2025) Safeguarding the Digital Consumer: A Comparative Legal and Psychological Analysis of Dark Patterns in E-Commerce. *Advances in Consumer Research*, 2 (4), 3567-3574

Received: 15 June 2025 Revised: 12 July 2025 Accepted:- 16 August 2025 Published: 30 August 2025

KEYWORDS
N/A

ABSTRACT
The rapid growth of e-commerce has transformed consumer markets, but alongside convenience has emerged the troubling phenomenon of "dark patterns" deceptive user interface designs that manipulate consumer decision-making. These patterns exploit cognitive biases, nudge users into unintended purchases or subscriptions, and erode consumer autonomy. This paper undertakes a comparative legal and psychological analysis of dark patterns, examining their prevalence, the vulnerabilities they exploit, and the effectiveness of regulatory responses. Drawing on legal frameworks in the United States, European Union, and India, it explores how consumer protection and data privacy laws have attempted to counter manipulative practices. Parallelly, insights from behavioural psychology demonstrate how heuristics such as scarcity bias, default bias, and loss aversion are systematically weaponized in digital marketplaces. While legal measures exist, enforcement is fragmented and often lags behind evolving technological designs. Psychological studies suggest that consumer awareness alone is insufficient, as manipulative designs operate subconsciously. The paper argues that safeguarding digital consumers requires a dual strategy—strengthening legal standards and incorporating behavioural insights into regulatory design. By bridging law and psychology, this study highlights pathways for more ethical e-commerce practices and proposes measures for policymakers, businesses, and consumer advocates to curb the proliferation of dark patterns.

1. INTRODUCTION

E-commerce has emerged as the dominant mode of retail in the digital age, offering unprecedented convenience, access, and personalization. Consumers can browse, compare, and purchase goods or services with a few clicks, revolutionizing traditional market structures. Yet, this digital revolution is not without risks. The virtual environment of online platforms is carefully engineered, not merely to display information but to influence behavior. Increasingly, businesses deploy "dark patterns" a term coined by Brignull (2010) to describe manipulative design features that intentionally steer users toward decisions that benefit the business, often at the expense of consumer interests.

Dark patterns exploit psychological vulnerabilities, such as cognitive overload, limited attention, and reliance on heuristics (Nouwens et al., 2020). Examples range from pre-ticked subscription boxes, misleading countdown timers, and disguised advertisements to complicated opt-out processes. These practices undermine consumer autonomy by nudging individuals toward actions they may not have taken under conditions of transparency and fairness. The cumulative impact is profound: consumers face financial loss, erosion of privacy, and diminished trust in digital marketplaces (Mathur et al., 2019).

Legal systems have responded with varying intensity. The European Union has taken a strong stance through the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA), while the United States has relied heavily on the Federal Trade Commission (FTC) to police unfair and deceptive practices (Helberger et al., 2021). In India, dark patterns have only recently entered regulatory discourse through the Consumer Protection Act and draft guidelines issued in 2023 (CCPA, 2023).

This paper adopts a comparative lens to examine how law and psychology intersect in addressing dark patterns. By analyzing both regulatory frameworks and the behavioral mechanisms underpinning consumer manipulation, it seeks to provide a holistic understanding of the problem and to chart practical pathways toward safeguarding the digital consumer.

2. STATEMENT OF PROBLEM

The emergence of dark patterns in e-commerce poses a significant threat to consumer welfare and market fairness. Unlike traditional forms of deception, these manipulative practices are embedded in the very architecture of digital platforms, making them harder to detect and regulate (Luger & Urquhart, 2020). They exploit unconscious biases and cognitive shortcuts, rendering consumers vulnerable even when they are informed and technologically literate. The legal challenge lies in defining the boundaries between persuasive design and unlawful manipulation, as well as ensuring enforcement in a rapidly evolving technological environment. Existing regulations often lag behind, leaving consumers exposed to subtle but impactful forms of exploitation (Helberger et al., 2021). Moreover, psychological insights demonstrate that awareness campaigns alone are insufficient, as manipulation frequently occurs below the threshold of conscious control (Tversky & Kahneman, 1974). The central problem, therefore, is how to effectively safeguard digital consumers from dark patterns through a combination of robust legal standards and behavioral science-informed regulatory strategies.

3. LITERATURE REVIEW

Scholarly engagement with dark patterns has grown steadily over the past decade, reflecting increasing concern over their role in undermining consumer rights. Brignull's (2010) foundational work identified and categorized dark patterns, ranging from "roach motels" (easy entry but difficult exit from services) to "sneak into basket" designs. His taxonomy sparked legal, ethical, and psychological inquiries into the phenomenon.

From a legal perspective, several studies highlight the fragmented nature of regulatory approaches. In the European Union, scholars have examined how the GDPR addresses manipulative consent mechanisms, with Nouwens et al. (2020) demonstrating that most cookie banners deploy dark patterns to nudge users toward data-sharing. The DSA (2022) further expands consumer protection by prohibiting manipulative design. By contrast, the U.S. relies on case-by-case enforcement through the FTC, with significant cases such as *FTC v. Amazon* (2023) revealing the limitations of existing laws in addressing subscription traps. In India, literature is nascent, with commentators noting that the Consumer Protection Act (2019) provides general safeguards but lacks explicit provisions on interface design. Draft guidelines on dark patterns (CCPA, 2023) signal growing awareness, though enforcement mechanisms remain underdeveloped.

Psychological literature complements these legal discussions by exploring how dark patterns exploit cognitive biases. Tversky and Kahneman's (1974) pioneering work on heuristics—such as default bias, scarcity, and loss aversion—provides a framework for understanding consumer vulnerability. Mathur et al. (2019) empirically analyzed hundreds of e-commerce websites and found widespread use of design tricks exploiting these biases. Notably, they argue that such manipulations are effective precisely because they target subconscious decision-making processes. Further research emphasizes that even informed consumers struggle to resist these nudges, indicating that information disclosure alone is insufficient for protection (Luger & Urquhart, 2020).

Interdisciplinary studies have begun bridging the gap between law and psychology. Luger and Urquhart (2020) argue for embedding behavioral insights into regulatory design, suggesting that regulators should anticipate consumer vulnerabilities rather than merely punishing businesses post-facto. Comparative analyses, such as Helberger et al. (2021), highlight the importance of aligning legal frameworks with empirical evidence of consumer harm.

Despite progress, several gaps remain. Most legal scholarship is jurisdiction-specific, with limited comparative analysis of how different regulatory systems confront dark patterns. Psychological studies often focus on experimental contexts, raising questions about external validity in real-world e-commerce. Moreover, few works examine how law and psychology can be integrated to produce holistic regulatory strategies.

3.1 A Taxonomy of Deception: Categorizing Dark Patterns in E-Commerce

To effectively analyse and regulate dark patterns, it is essential to first establish a clear and comprehensive taxonomy of their various forms. The term, first catalogued by Brignull, encompasses a wide range of manipulative interface designs. Subsequent academic research and regulatory investigations have expanded and refined this classification, identifying recurring strategies that e-commerce platforms use to influence consumer behaviour. These patterns can be broadly grouped into categories based on the type of psychological vulnerability they exploit or the deceptive function they perform. The following table synthesizes the primary types of dark patterns documented in the literature, providing definitions, the underlying psychological principles they leverage, and concrete examples from real-world e-commerce platforms.

Table 1: A Comprehensive Taxonomy of Dark Patterns in E-Commerce

Dark Pattern Category	Dark Pattern Type	Definition	Psychological Principle Exploited	E-Commerce Example (with citations)
Obstruction	Roach Motel / Subscription Trap	Designing a process that is easy to enter (e.g., sign up) but difficult to exit (e.g., cancel).	Status Quo Bias, Cognitive Load	Amazon's multi-step Prime cancellation process, internally nicknamed "Iliad" for its epic length.
Sneaking	Sneak into Basket	Adding items to a user's cart without their explicit consent, often via a pre-checked box.	In attentional Blindness, Default Bias	Sports Direct adding a "free" mug with a £1 delivery charge to baskets ; Avas Flowers adding a greeting card.
	Hidden Costs / Drip Pricing	Revealing previously undisclosed charges (e.g., taxes, service fees) only at the final step of the checkout process.	Sunk Cost Fallacy, Anchoring Bias	Airlines hiding baggage fees until the final payment screen.
Urgency	False Urgency / Scarcity	Creating a false sense of limited availability or time to rush a purchasing decision.	Scarcity Heuristic, Fear of Missing Out (FOMO)	Countdown timers that reset on page reload; "Only 2 left in stock!" messages that appear for all products.
Misdirection	Visual Interference / False Hierarchy	Using visual design (e.g., color, size, placement) to nudge users toward a preferred option and away from their intended action.	Attentional Bias	Delta's check-in screen using a prominent red button for an upgrade and a less conspicuous grey button to decline.
Social Proof	Fake Social Proof	Fabricating or exaggerating the popularity of a product through fake reviews, testimonials, or activity messages.	Bandwagon Effect, Authority Bias	"32 people purchased this in the last hour" messages that are programmed to appear on a recurring schedule.
Forced Action	Forced Continuity	Automatically converting a free trial to a paid subscription without adequate notice or a simple cancellation mechanism.	Default Bias, Procrastination	Many streaming services and software trials that require credit card details upfront and auto-renew silently.

3.2 The Psychology of Persuasion vs. Manipulation

The effectiveness of dark patterns is rooted in their exploitation of fundamental principles of human psychology. It is crucial, however, to distinguish between legitimate persuasion and illicit manipulation. Benign persuasive design, often referred to as "nudging," aims to help consumers overcome decision-making biases in ways that are welfare-enhancing and align with their long-term interests. For example, a website might default to a double-sided printing option to encourage environmental conservation. In contrast, the principal purpose of dark patterns is to complicate or obscure consumer decision-making in a way that directly benefits the seller, often at the consumer's expense. They are designed to be manipulative rather than persuasive, encouraging users to make decisions they would not have made if not for the interface's influence.

Dark patterns achieve this by targeting well-documented cognitive biases and heuristics—the mental shortcuts that the human brain uses to process information and make decisions efficiently. Dark patterns exploit our mental shortcuts to push us into choices we might not really want. Scarcity tricks, like countdown timers or low-stock alerts, create fake urgency. Confirm-shaming plays on loss aversion by making rejection feel like a loss. And pre-checked boxes or auto-renewals tap into our tendency to stick with the default rather than exert effort to opt out. Social proof and authority bias are abused with the use of fake testimonials or exaggerated counters to create a feeling of trust or popularity to trigger the bandwagon effect. Again, these methods take advantage of consumers' rational decision-making process, and funnel consumers towards choices that are driven by psychological pressure instead of actual intention.

3.3 Quantifying the Threat: Empirical Studies on Prevalence and Impact

Dark patterns are not an isolated issue limited to a small niche of the web. Rather, empirical research has shown that dark patterns occur widely and consistently across the e-commerce sector. For example, a landmark study at Princeton University and the University of Chicago conducted a large-scale study of nearly 11,000 shopping websites, finding over 11% more than 1,200 sites employed dark patterns. The study found that dark patterns are especially common on popular websites, exposing millions of users to manipulation. They are even more widespread in mobile apps, according to a 2022 European Commission report, 97% of leading apps contained at least one deceptive design. Similarly, a 2024 global review by the International Consumer Protection and Enforcement Network (ICPEN) showed that 76% of websites used at least one dark pattern, with 67% using several.

Dark patterns have negative implications on an economic and psychological level, as well as inject harm into a social context that erodes trust in digital commerce. Economically, dark patterns lead to unwanted purchases, hidden charges (also known as "drip pricing"), forced continuity, and more. One study estimated unwanted purchases from dark patterns cost the average American family at least $3,200 annually, and over 40% of online shoppers reported experiencing unplanned financial consequences from dark patterns. Psychologically, consumers exposed to dark patterns that encourage deception, often report feeling frustration, anxiety, guilt, and even a sense of betrayal; these negative psychological implications can affect brand loyalty – one survey reported that 43% of shoppers abandoned the retailer due to dark patterning. In addition to consumers experiencing financial and emotional harm from dark patterns, there are also serious privacy implications - through tactics such as “Privacy Zuckering,” confusing interfaces, or consent by default mechanisms that persuade consumers to share more data than they intended. In total, dark patterns show that consumers are facing not only individual, isolated design flaws, but a systemic blight on all of e-commerce that distorts consumer choice, drains economic resources, weakens privacy protections, and compromises long-term trust in the digital economy.

4. RESEARCH GAP

Although significant scholarship exists on both the legal and psychological dimensions of dark patterns, critical gaps remain. First, much of the legal literature is jurisdiction-specific, examining either European, American, or Indian contexts in isolation. A comparative analysis that systematically evaluates the strengths and weaknesses of these frameworks is lacking (Helberger et al., 2021). Second, psychological studies have richly documented the biases exploited by dark patterns, but they often stop short of translating these insights into actionable regulatory strategies (Mathur et al., 2019). The disconnect between empirical findings in psychology and normative frameworks in law limits the effectiveness of consumer protection. Third, while recent regulations acknowledge dark patterns, enforcement mechanisms are underexplored, particularly in developing economies where digital literacy varies widely (CCPA, 2023). Finally, scholarship rarely considers how law and psychology can be integrated into a unified framework for safeguarding consumers. This research addresses these gaps by adopting a comparative, interdisciplinary approach, demonstrating how behavioral science can inform legal design and how diverse jurisdictions can learn from one another to regulate dark patterns more effectively.

5. ANALYSIS

5.1 Methodology

This study employs a comparative and interdisciplinary methodology. It draws upon doctrinal legal analysis of statutory instruments, case law, and regulatory guidelines in the European Union, United States, and India. Alongside, it incorporates insights from behavioral psychology and empirical consumer research to explain how dark patterns exploit human cognition. Secondary sources—including academic studies, regulatory reports, consumer surveys, and enforcement cases—are

examined. The interdisciplinary approach allows identification of regulatory strengths and weaknesses while situating them in the psychological realities of consumer decision-making. This analysis employs a comparative legal methodology to critically evaluate the regulatory frameworks governing dark patterns in the United States and the European Union. The approach involves an examination of primary legal sources, including federal and state statutes in the U.S. (e.g., the FTC Act, ROSCA, CPRA) and E.U. regulations and directives (e.g., the GDPR, DSA, UCPD). This is supplemented by an analysis of secondary sources, such as significant case law, regulatory guidance documents (e.g., the FTC's "Bringing Dark Patterns to Light" report), and major enforcement actions against prominent e-commerce companies. The legal analysis is contextualized through a qualitative synthesis of the empirical data on the prevalence, psychological mechanisms, and consumer impact of dark patterns, as established in the literature review. The effectiveness of each legal model is assessed against several key criteria: the clarity and scope of its prohibitions, the robustness and consistency of its enforcement mechanisms, and its adaptability to emerging technological challenges, particularly the rise of AI-driven manipulation.

5.2 Legal Analysis

5.2.1 European Union (EU).

The EU is regarded as the most advanced jurisdiction in regulating dark patterns. The **General Data Protection Regulation (GDPR)** requires consent to be freely given, informed, and unambiguous. Empirical research shows that compliance remains limited: Nouwens et al. (2020) analyzed 1,000 EU websites and found that **over 90% of cookie banners employed at least one dark pattern**, such as nudging users toward “accept all.” The **Digital Services Act (DSA, 2022)** directly prohibits manipulative interfaces. Yet enforcement varies. For example, in 2022, France’s CNIL fined Google €150 million and Facebook €60 million for making cookie refusal harder than acceptance. These penalties demonstrate strong regulatory intent, but fragmented enforcement across member states remains a challenge.

5.2.2 United States (US).

The U.S. takes a case-by-case approach under **Section 5 of the Federal Trade Commission (FTC) Act**. In 2021, the FTC issued an enforcement policy statement warning firms against “illegal dark patterns.” Empirical findings suggest widespread issues: a Princeton University study found **1,818 instances of dark patterns across 1,200 popular U.S. websites** (Mathur et al., 2019). High-profile cases illustrate this trend: in *FTC v. ABCMouse* (2020), the company paid $10 million for trapping consumers in subscriptions; in *FTC v. Amazon* (2023), the company was accused of using deceptive interfaces to enroll millions into Prime without consent. However, the lack of explicit statutory provisions means businesses operate in regulatory grey zones until enforcement is triggered. The FTC's primary weapon against dark patterns is Section 5 of the FTC Act, a law enacted in 1914 that grants the agency broad authority to prohibit "unfair or deceptive acts or practices in or affecting commerce". The FTC has interpreted this mandate to apply to manipulative online interface designs. In its influential 2022 staff report, "Bringing Dark Patterns to Light," the agency defined dark patterns as "design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm". The report outlines four main categories of concern: design elements that induce false beliefs (e.g., disguised ads), that hide or obscure material information (e.g., junk fees), that lead to unauthorized charges (e.g., subscription traps), and that subvert privacy choices.

In addition to the general authority of the FTC Act, the agency also enforces more specific statutes, most notably the Restore Online Shoppers' Confidence Act (ROSCA). Enacted in 2010, ROSCA directly targets "negative option" features, a common form of dark pattern. The law makes it illegal to charge consumers for goods or services sold online through a negative option plan unless the seller: (1) clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer's billing information; (2) obtains the consumer's express informed consent before making the charge; and (3) provides a simple, easy-to-use mechanism for the consumer to stop recurring charges.

5.2.3 India.

India is in the early stages of developing specific responses. The **Consumer Protection Act (2019)** and e-commerce rules prohibit misleading advertisements and unfair trade practices, but they do not directly mention interface design. Recognizing this gap, the **Central Consumer Protection Authority (CCPA)** issued draft guidelines in 2023 identifying 13 specific dark patterns, including drip pricing, false urgency, and basket sneaking. Surveys indicate the urgency of such regulation: a 2022 Local Circles consumer poll reported that **70% of Indian online shoppers had experienced drip pricing**, where additional charges are revealed only at checkout. Implementation challenges remain due to limited digital literacy (only **38% of Indian internet users are “digitally confident,” according to IAMAI, 2022**) and weak enforcement infrastructure.

5.3 Psychological Analysis

Dark patterns are effective because they exploit **predictable cognitive biases**. Data confirms their impact:

i. **Scarcity bias:** Expedia and Booking.com were fined in 2020 by the UK Competition and Markets Authority after research showed that “only 2 rooms left” notices increased bookings by **over 15%**, even when scarcity was fabricated.

ii. **Default bias:** A European Commission (2022) study found that **56% of consumers stuck with default options** (e.g., pre-checked subscription boxes) even when alternatives were better.

iii. **Loss aversion:** Countdown timers increase purchase likelihood. In controlled experiments, users exposed to "limited time offer" messages were **twice as likely to buy** compared to a control group (Mathur et al., 2019).

Even technologically literate users are vulnerable. A Harvard Business Review survey (2021) revealed that **42% of U.S. consumers admitted to regretting online purchases made under time-limited or manipulative design conditions.** These findings confirm that disclosure-based interventions alone (e.g., longer terms and conditions) are insufficient, as manipulation often bypasses conscious awareness.

5.4 Comparative Insights

A cross-jurisdictional comparison yields important insights:

i. **European Union**: Proactive ban-based approach; regulators impose heavy fines but face challenges in harmonization. Despite GDPR, **non-compliance with fair consent remains above 80%** in many sectors (Nouwens et al., 2020).

ii. **United States**: Enforcement-driven approach; highly dependent on FTC litigation. While visible cases exist, dark patterns remain rampant, with studies showing **11% of e-commerce sites deploy at least one dark pattern at scale** (Mathur et al., 2019).

iii. **India**: Preventive intent but weak infrastructure. Draft guidelines are promising, yet **low consumer awareness (60% of users cannot identify manipulative design, IAMAI 2022)** hinders effectiveness.

From a psychological standpoint, only the EU's proactive ban sufficiently anticipates consumer vulnerabilities, while the U.S. and India remain reactive.

5.5 Challenges and Implications

The major challenges include:

a) **Definitional ambiguity:** Drawing the line between persuasive nudging (e.g., highlighting eco-friendly choices) and exploitative dark patterns is contentious.

b) **Global enforcement:** E-commerce is cross-border. A study by BEUC (2022) noted that **67% of manipulative practices were deployed by multinational platforms**, requiring global cooperation.

c) **Over-reliance on consumer choice:** Evidence shows disclosures fail; **average consumers spend only 13 seconds on consent screens** (Nouwens et al., 2020).

d) **Innovation vs. protection trade-off:** Excessive regulation may deter legitimate personalization, while under-regulation perpetuates consumer harm.

5.6 Synthesis

The analysis demonstrates that effective consumer protection requires integrating **legal prohibitions with behavioral science insights**. Laws must recognize that consumers are not fully rational actors but are predictably irrational (Tversky & Kahneman, 1974). Regulation should therefore move away from disclosure-heavy models and adopt **structural safeguards**, such as banning default opt-ins, mandating clear unsubscribe buttons, and prohibiting fabricated scarcity cues.

Data from EU fines, U.S. enforcement cases, and Indian consumer surveys collectively underscore the scale of the problem and highlight that only proactive, behaviorally informed regulation can meaningfully safeguard consumers.

6. CONCLUSION

Existing research has advanced our understanding of dark patterns by identifying and classifying their presence in static and semi-static interfaces. Taxonomies in this field remain valuable for mapping the current landscape of digital manipulation. However, a critical gap is emerging with the rise of artificial intelligence (AI) and machine learning. The next generation of dark patterns will be dynamic and personalized, adapting in real time to an individual's behavior, psychological traits, and vulnerabilities. For example, an AI system might detect hesitation through mouse movements and immediately deploy a tailored scarcity prompt or social proof cue. Such manipulations are transient, individualized, and continuously evolving, which makes them exceptionally difficult to detect, document, or prove. Traditional research methods—manual website sweeps, A/B testing, or static code analysis—are ill-suited to capture this phenomenon, leaving a substantial blind spot. As a result, existing regulatory frameworks, such as the EU's Digital Services Act (DSA) and California's Consumer Privacy Rights Act (CPRA), which target fixed design features, may be inadequate to address this emerging frontier of algorithmic deception. However, when the manipulative agent is a fluid, adaptive algorithm, the problem's locus shifts. It becomes exceedingly difficult to prove that a specific design is a dark pattern when that design is unique to each user and interaction. The manipulative intent is embedded within the algorithm itself. This points to a crucial area for future research and regulatory development. The focus must expand from auditing the final visual output of a website to developing methods for

auditing the underlying algorithms for manipulative potential. This may require a paradigm shift from banning specific patterns to regulating the outcomes and processes of algorithmic personalization systems, placing a burden on companies to demonstrate that their algorithms are not deceptively manipulative. Such a move would align with broader efforts to establish a "trustworthy AI" framework and apply its principles directly to the e-commerce environment. The proliferation of dark patterns in e-commerce reflects the intersection of business incentives, technological design, and human psychology. By embedding manipulative tactics within user interfaces, companies exploit consumer vulnerabilities, leading to financial harm, privacy erosion, and declining trust in digital markets (Mathur et al., 2019). Legal systems have begun responding, but their approaches vary. The European Union's proactive prohibition model demonstrates recognition of consumer psychology, while the U.S. continues to rely on reactive enforcement through the FTC (Helberger et al., 2021). India, though late to the discourse, has taken important steps by drafting guidelines against dark patterns (CCPA, 2023).

Yet, regulation alone is insufficient if it does not account for psychological realities. Consumers cannot always resist manipulative nudges, even when aware of them, as biases such as default inertia and scarcity heuristics operate subconsciously (Tversky & Kahneman, 1974). This highlights the need for regulatory frameworks that move beyond disclosure and place substantive limits on design practices. The integration of behavioral insights into law is therefore not optional but necessary for effective consumer protection.

Ultimately, safeguarding the digital consumer requires a balance: fostering innovation in e-commerce while curbing harmful manipulation. A comparative and interdisciplinary approach underscores that while legal prohibitions are essential, they must be informed by psychology to address the root mechanisms of exploitation. Only through such synergy can consumer autonomy and trust be preserved in the digital marketplace.

7. SUGGESTIONS

To effectively safeguard digital consumers against dark patterns, several measures are necessary. First, legal frameworks should adopt explicit prohibitions on manipulative design, as seen in the European Union, rather than relying solely on broad principles of fairness or deception. Countries like India should build on their draft guidelines to enact enforceable statutory provisions (CCPA, 2023).

Second, regulators must incorporate behavioral insights into enforcement. Recognizing that consumers are not fully rational actors, policies should target the structural features of dark patterns rather than assuming informed choice suffices (Luger & Urquhart, 2020). For example, banning pre-ticked boxes or mandating simple unsubscribe mechanisms directly addresses psychological vulnerabilities.

Third, enforcement capacity must be strengthened. Regulatory bodies require technical expertise to detect dark patterns and authority to impose meaningful penalties. Cross-border collaboration is equally vital, given the global nature of e-commerce platforms (Helberger et al., 2021).

Fourth, consumer education should complement regulation. Awareness campaigns highlighting common dark patterns can empower individuals, though such strategies should be seen as supplementary, not primary, tools.

Finally, ethical design standards should be encouraged within industry. Companies should be incentivized to adopt transparency and user-centric practices, thereby fostering trust and long-term consumer loyalty. Together, these strategies can create a fairer, more trustworthy digital marketplace.

REFERENCES

[1] Brignull, H. (2010). Dark patterns: User interfaces designed to trick people. Retrieved from https://www.darkpatterns.org

[2] Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

[3] Mathur, A., Acar, G., Friedman, M. G., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1–32. https://doi.org/10.1145/3359183

[4] Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW), 1–24. https://doi.org/10.1145/3397884

[5] Luger, E., & Urquhart, L. (2020). A critical reflection on the deployment of dark patterns in digital platforms. Technology in Society, 63, 101417. https://doi.org/10.1016/j.techsoc.2020.101417

[6] Helberger, N., Araujo, T., & de Vreese, C. H. (2021). Who is the fairest of them all? Public attitudes and expectations of algorithmic transparency. Policy & Internet, 13(1), 64–86. https://doi.org/10.1002/poi3.238

[7] Digital Services Act. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council.

[8] Federal Trade Commission (FTC) v. Amazon.com, Inc., No. 2:23-cv-0932 (W.D. Wash. 2023).

[9] Central Consumer Protection Authority (CCPA). (2023). Draft guidelines for prevention and regulation of dark patterns. Government of India.

[10] FTC. (2022). FTC report shows rise in sophisticated dark patterns designed to trick and trap consumers. Retrieved from https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers

[11] European Parliament. (2022). Dark patterns: Impact on consumers and potential harm. BEUC presentation at IMCO Hearing, March 16, 2022.

[12] Rasenberger, R. (2024). Protecting consumers from the dark. The Regulatory Review. Retrieved from https://www.theregreview.org

[13] Cambridge University Press. (2022). Dark patterns and consumer vulnerability. Behavioural Public Policy. https://doi.org/10.1017/bpp.2022.18

[14] Xigen. (2022). The Dark Patterns Report. Retrieved from https://xigen.co.uk/reports/the-dark-patterns-report/

[15] OECD. (2024). Six “dark patterns” used to manipulate you when shopping online. Retrieved from https://www.oecd.org

[16] UNCTAD. (2020). E-Commerce and Consumer Protection. Retrieved from https://unctad.org

[17] Narayanan, A., et al. (2021). Bringing dark patterns to light: Policy and enforcement challenges. Princeton Web Transparency Project.

[18] Didomi. (2023). What are dark patterns? (with examples). Retrieved from https://www.didomi.io/blog/what-are-dark-patterns