The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DARK PATTERNS IN DIGITAL PLATFORMS: CONSUMER MANIPULATION OR LEGITIMATE BUSINESS STRATEGY? LEGAL IMPLICATIONS UNDER CYBER AND CONSUMER PROTECTION LAWS

~ Akanksha Choudhary

Introduction

Dark patterns describe design practices in websites and apps that deliberately steer users toward actions they otherwise might not take. These practices often include hiding important information, misleading buttons, or presenting an option to opt-out in a way that is ambiguous or takes disproportionate effort that encourages the user to choose an outcome that benefits the platform or service and not the user. Some examples are commonly encountered in our lives using digital platforms: e-commerce websites will sneak charges at checkout and alter delivery dates if the customer does not overtly monitor it, social media platforms might make it difficult to configure privacy settings, and subscription services may use false prompts conveying misleading assignments for users to confirm auto-renewal.[1]

The importance of studying dark patterns is important because technology plays a role in everyday life. Every day, users perform online tasks such as shopping, banking, entertainment, and communication potentially without realizing how design is invisibly shaping their decisions. By exploiting cognitive biases and human psychology through the use of dark patterns technology providers are profiting by, in essence, stealing informed consent; this raises significant ethical concerns and potentially legal dilemmas.[2]

This research aims to determine whether dark patterns are simply aggressive business tactics or whether they are manipulating the consumer in a manner that requires intervention. Our consideration will be entirely focused on India's legislative framework, including the Consumer Protection Act and the Information Technology Act, 2000, along with learning from other parts of the world including the EU and the General Data Protection Regulation (GDPR) and the US Federal Trade Commission (FTC) practices. We will attempt to determine whether there is adequate law to protect consumers in India or if there should be

laws in place prohibiting manipulative and deceptive behaviour in the digital world.

Understanding Dark Patterns

There are many types of dark patterns and they each, in their own way, are designed to impact user behavior and limit informed choice. From Harry Brignull's also referenced taxonomy, these manipulative techniques come in many recurring forms. Bait and switch attracts users with one offer and delivers another, usually, less appealing offer. Sneak into basket somehow adds items or services to the cart without the user's full agreement. Roach motel makes it too easy to subscribe to a service and too hard to unsubscribe or opt out. Privacy Zuckering deceives users into providing more personal data than is intended and obfuscation offers intent on providing minimal or less information making actions like deleting accounts, and refund requests frustratingly complicated and confusing.[3]

These dark patterns often use psychological manipulation to enhance use. In manipulating cognition, it is common to use urgency, scarcity or social proofing to push users to act in a way that is contrary to what they would have otherwise acted upon. Even minute design elements or choices like button placement, or the use of pre-checked boxes can tip the edge in reducing the space for unconstrained choice.

Consumers are greatly impacted. Dark patterns erode trust in digital platforms, channel cognitive biases, and diminish autonomy, in effect moving the power from the individual to the service provider. What seems like a regular online experience whether it be making a purchase, signing up for a newsletter, or adjusting privacy settings can become a sequence of manipulative nudging for the benefit of the company at the expense of the user. The first steps towards understanding the ethical and legal considerations facing such patterns is naming and identifying them, as digital transactions continue to take a more prominent place in our everyday lives.

Legal Landscape: India

In India, the legal framework addressing manipulative digital practices such as dark patterns primarily draws on the **Consumer Protection Act, 2019 (CPA 2019)** and the **Information Technology Act, 2000 (IT Act)**, complemented by rules and guidelines for e-commerce and intermediaries.

The CPA 2019 broadens the concept of **unfair trade practices** to explicitly cover misleading representations, deceptive marketing, and manipulative tactics that exploit consumers' trust.

Sections such as **Section 2(47)** define unfair trade practices in ways that can encompass dark patterns, particularly when users are coerced into purchases, forced subscriptions, or misled by interface design. The law extends to **digital platforms and online transactions**, ensuring that e-commerce operators, social media platforms, and subscription services fall within its ambit. The **Consumer Protection (E-Commerce) Rules, 2020** further reinforce these protections by requiring transparency in pricing, clear disclosure of terms, and obligations for grievance redressal mechanisms, which indirectly curb some forms of dark patterns like hidden charges or obfuscated cancellation options.

Complementing this, the IT Act 2000 addresses **misrepresentation, data privacy, and intermediary liability**. While Sections 43A and 66E protect users' sensitive data from misuse, and Section 66D penalizes cheating by impersonation, these provisions can be invoked in cases where dark patterns trick users into sharing personal information or making unintended payments. The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** place obligations on digital intermediaries to exercise due diligence, respond to consumer complaints, and ensure transparency in user interface and experience. These rules, while not explicitly targeting dark patterns, create regulatory pressure for platforms to avoid manipulative UI/UX practices.

Several real-world examples in India illustrate these legal issues. E-commerce platforms have faced complaints for **misleading pricing, pre-selected subscriptions, or hidden add-on services** that exploit consumers' attention and trust. Complaints have been filed with **Consumer Forums and the National Consumer Disputes Redressal Commission (NCDRC)**, highlighting the practical challenges of holding companies accountable. Although some complaints have resulted in refunds or penalties, enforcement remains sporadic, and many cases rely on consumers recognizing the manipulation rather than proactive monitoring by regulators.

Overall, India's legal framework offers a foundation to address dark patterns, but gaps remain. While consumer protection laws and IT provisions cover certain deceptive practices, there is **no explicit recognition of manipulative UI/UX tactics as a distinct category of unfair trade practices**, leaving much of the regulatory burden on interpretation and judicial discretion. Strengthening these laws and providing clearer guidelines could ensure more consistent protection for digital consumers.

Ethical and Business Perspectives

Dark patterns sit at the intersection of business strategy and ethical concern, sparking debate over whether they are legitimate tools for growth or forms of consumer exploitation. From a business standpoint, these design techniques can significantly boost **conversion rates**, increase subscriptions, and drive revenues. By subtly nudging users toward desired actions such as completing purchases, opting into services, or sharing personal data companies argue that they are simply optimizing user engagement in a competitive digital market.[4]

However, the counter-argument is compelling. Dark patterns erode **consumer trust**, compromise autonomy, and often mislead users into decisions they would not otherwise make. Beyond ethical concerns, manipulative designs expose companies to **legal and reputational risks**, particularly under consumer protection and cyber laws. Users who feel deceived may abandon platforms, leaving long-term damage that outweighs short-term gains.

Ethical analysis of dark patterns can be informed by classical theories. From a **deontological perspective**, manipulative UI/UX is inherently wrong because it violates the principle of treating individuals as autonomous agents capable of informed choice. In contrast, a **utilitarian perspective** might weigh the overall benefits, asking whether the aggregate gains for businesses justify the manipulation of individual users a position that is difficult to defend given the harm to privacy, trust, and long-term societal welfare.

Ultimately, the ethical debate underscores that business efficiency and profitability must be balanced against respect for user autonomy and fairness. Companies cannot rely solely on technical sophistication or market pressures; they must design interfaces that are transparent, understandable, and ethically responsible.

Challenges in Regulating Dark Patterns

Regulating dark patterns presents a unique set of challenges due to the intersection of technology, law, and consumer behavior. One of the primary difficulties lies in **defining manipulation legally**. While dark patterns exploit psychological biases to nudge users into actions they might not otherwise take, businesses often frame these practices as standard marketing strategies. This creates a **gray area** where distinguishing between legitimate business practice and unethical manipulation becomes legally complex. Courts and regulators often struggle to draw precise boundaries, which can delay enforcement or lead to inconsistent judgments.

Another major challenge is the **rapid pace of technological innovation**. Digital platforms continually evolve their interfaces, employing new tactics to capture user attention or collect

data. Legal frameworks, in contrast, are inherently slower to adapt. Statutes drafted for older forms of digital commerce may fail to encompass the nuanced strategies of modern platforms, leaving regulators one step behind.

The **global nature of digital platforms** further complicates regulation. Dark patterns often originate from companies operating across borders, making **jurisdictional enforcement difficult**. Indian authorities may lack the legal reach to act against a platform headquartered abroad, while cross-border cooperation mechanisms are still underdeveloped.

Finally, there is a tension between **self-regulation and statutory regulation**. Many tech companies favor self-regulatory measures, such as internal ethics boards or voluntary transparency reports, but these often lack enforceability. Conversely, statutory interventions if too rigid risk stifling innovation or imposing compliance burdens on smaller firms. Balancing these approaches is crucial to ensure consumer protection while maintaining a vibrant digital economy.

In sum, the combination of definitional ambiguity, fast-paced technological change, cross-border enforcement challenges, and regulatory tension makes addressing dark patterns a particularly complex task for modern legal systems.

Recommendations

Addressing dark patterns requires a multi-pronged approach that combines **legal, technological, and educational strategies**. First, there is a need to **draft clear guidelines for ethical UX design**, setting boundaries on manipulative interface techniques and defining what constitutes deceptive practices. These guidelines should be developed in consultation with industry experts, behavioral scientists, and legal authorities to ensure they are both practical and enforceable.

Second, **strengthening consumer awareness and digital literacy** is crucial. Users should be educated about common dark patterns, the risks of unintended consent, and strategies to protect their personal data. Public campaigns, educational modules in schools and universities, and platform-driven awareness initiatives can empower consumers to make informed choices.

Third, **explicit consent clauses and transparent subscription or cancellation policies** should be mandated for all digital services. Interfaces must clearly communicate terms, fees, and opt- out procedures, reducing ambiguity and ensuring that users retain control over their digital engagements.

Finally, **proactive monitoring by authorities** is essential. Regulatory bodies should adopt models similar to the **California Consumer Privacy Act (CCPA)** or the **FTC's guidelines in the United States**, where authorities can audit platforms, investigate complaints, and impose penalties for violations. This oversight, combined with industry self-regulation, can incentivize companies to adopt user-friendly and ethical design practices.

By integrating these measures, India can create a legal and technological ecosystem that **protects consumers from manipulative practices** while fostering trust and innovation in the digital economy.

Conclusion

Dark patterns represent a growing challenge in the digital age, as they deliberately exploit cognitive biases to influence consumer behavior. By blurring the line between **aggressive marketing and manipulative practices**, these design strategies raise profound ethical and legal concerns. While technology companies continue to innovate, current legal frameworks in India remain **inadequate** to address the nuances of user interface manipulation, leaving consumers vulnerable to deception and involuntary consent.

The ethical implications are equally significant: dark patterns erode trust, compromise user autonomy, and disproportionately affect those with lower digital literacy. Addressing this issue, therefore, requires more than reactive enforcement; it calls for **proactive regulation, clear ethical guidelines, and consumer education**.

A balanced approach is essential one that **protects consumer rights** and promotes transparency, while allowing businesses to employ legitimate marketing strategies and maintain innovation. By combining legal reform, regulatory oversight, and digital literacy initiatives, India can create a digital ecosystem where consumers are empowered, companies are accountable, and trust in online platforms is strengthened.