Page: 190-214 URL: www.lijdlr.com

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.273

DARK PATTERNS IN E-COMMERCE: EVALUATING INDIA'S CONSUMER PROTECTION FRAMEWORK IN THE DIGITAL MARKETSPACE

J Janice Vinolia[1]

I. ABSTRACT

The rapid growth of e-commerce has transformed the way consumers purchase goods and services. Online platforms now offer convenience, competitive prices and easy access to a wide range of products. However, along with these advantages, many digital platforms have adopted certain website and application designs that influence or manipulate consumers into making decisions they may not have otherwise taken. These deceptive design practices, commonly known as dark patterns, affect consumer choice by creating false urgency, hiding important information, making cancellation difficult, or adding unwanted products and services during the purchasing process. Recognising the increasing misuse of such practices, India introduced the Guidelines for Prevention and Regulation of Dark Patterns, 2023 under the Central Consumer Protection Authority (CCPA). While these guidelines mark an important step towards protecting consumers, several concerns remain regarding their enforcement, implementation and effectiveness. Existing consumer protection laws were primarily drafted to regulate traditional unfair trade practices and do not fully address the challenges posed by digital interface manipulation. This paper examines the concept of dark patterns and analyses the adequacy of India's legal framework in regulating such practices. It evaluates the Consumer Protection Act, 2019, the Consumer Protection (E-Commerce) Rules, 2020, and the CCPA Guidelines, 2023. The paper also briefly compares India's approach with regulatory developments in the European Union, the United Kingdom and the United States. Based on this analysis, the paper identifies existing legal gaps and suggests practical reforms to strengthen consumer protection in India's growing digital marketplace. The study concludes that while India has taken a positive step by recognising dark patterns, stronger

[1] Final Year, B.A. LL.B. (Hons.), Saveetha School of Law, SIMATS, Chennai (India). Email ID: janivinolia@gmail.com

enforcement mechanisms and clearer legal obligations are necessary to ensure fair and transparent online commerce.

II. KEYWORDS

Dark Patterns, E-Commerce, Consumer Protection, Digital Marketplace, CCPA Guidelines.

III. INTRODUCTION

The digital economy has changed the way people shop, communicate and access services. Today, consumers can purchase almost anything with just a few clicks through online marketplaces and mobile applications. The growth of e-commerce has created greater convenience, wider choices and competitive pricing, making online shopping an essential part of everyday life. However, alongside these benefits, digital platforms have increasingly begun using interface designs that influence consumers' decisions in subtle and often misleading ways.

These manipulative interface designs are commonly referred to as dark patterns. They are designed to encourage users to make choices that benefit the platform rather than the consumer. Examples include displaying fake countdown timers to create a false sense of urgency, automatically adding products to a shopping cart, making subscription cancellation unnecessarily complicated, or hiding additional charges until the final stage of payment. Although these practices may appear to be minor design features, they can significantly affect consumer autonomy and informed decision-making.

The growing use of dark patterns has raised important legal and ethical concerns across the world. Since consumers often remain unaware that they are being influenced, traditional consumer protection laws are not always sufficient to address these practices. Recognising this issue, the Central Consumer Protection Authority (CCPA) issued the

Guidelines for Prevention and Regulation of Dark Patterns, 2023[2], identifying various forms of deceptive online practices and prohibiting their use in digital commerce.

Despite this development, questions remain regarding whether India's present legal framework provides adequate protection against such manipulative practices. Effective regulation requires not only clear legal provisions but also proper enforcement, consumer awareness and accountability of digital platforms. This paper therefore examines the existing legal framework governing dark patterns in India and evaluates whether it is capable of protecting consumers in today's rapidly evolving digital marketplace.

A. Research Problem

The increasing use of dark patterns in digital commerce has created a significant challenge for consumer protection in India. Although the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 prohibit unfair trade practices, they were enacted before dark patterns became a major concern in online transactions. As a result, many manipulative interface designs continue to operate in a legal grey area.

The introduction of the CCPA Guidelines in 2023 is a welcome initiative, but these guidelines alone may not be sufficient to effectively regulate all forms of deceptive digital practices. Issues relating to enforcement, monitoring, consumer awareness and regulatory accountability continue to exist. Therefore, there is a need to examine whether India's present legal framework adequately protects consumers from dark patterns and what improvements are necessary to strengthen digital consumer rights.

B. Research Objectives

The present study seeks to achieve the following objectives:

1. To understand the concept and different forms of dark patterns used in e-commerce platforms.

---

[2] *id.*

 (ISSN: 2583-7753)

2. To examine the legal framework governing dark patterns in India, with particular reference to the Consumer Protection Act, 2019, the Consumer Protection (E-Commerce) Rules, 2020 and the CCPA Guidelines, 2023.
3. To analyse whether the existing legal framework adequately protects consumers from deceptive online practices.
4. To compare India's approach with selected international jurisdictions and identify best practices.
5. To suggest legal and policy measures for strengthening consumer protection in the digital marketplace.

C. Research Questions

The study is based on the following research questions:

1. What are dark patterns and how do they influence consumer decision-making in e-commerce?
2. Does the existing legal framework in India effectively regulate dark patterns?
3. What challenges do regulatory authorities face in preventing deceptive online practices?
4. How have other countries addressed the issue of dark patterns?
5. What reforms can improve consumer protection in India's digital marketplace?

D. Research Hypothesis

1. **Null Hypothesis:** The existing legal framework in India is sufficient to regulate dark patterns and adequately protect consumers in the digital marketplace.
2. **Alternative Hypothesis:** The existing legal framework in India is not sufficient to effectively regulate dark patterns, and stronger legal and regulatory measures are required to protect consumers.

E. Research Methodology

This research follows a doctrinal research methodology, as it is primarily based on the study and analysis of existing laws, judicial decisions, government guidelines, books, journal articles and other secondary sources. The research examines statutory provisions relating to consumer protection and digital commerce to understand how dark patterns are presently regulated in India.

The study mainly relies upon the Consumer Protection Act, 2019, the Consumer Protection (E-Commerce) Rules, 2020 and the Guidelines for Prevention and Regulation of Dark Patterns, 2023 issued by the Central Consumer Protection Authority (CCPA). It also refers to international legal developments in jurisdictions such as the European Union, the United Kingdom and the United States to provide a comparative understanding of the subject.

The research adopts an analytical and comparative approach to identify gaps in the existing legal framework and to evaluate whether the current regulatory measures are sufficient to address deceptive digital practices. The study is entirely based on secondary data and does not involve any field survey or empirical research.

F. Literature Review

Several scholars, regulatory authorities and international organisations have examined the growing concern of dark patterns and their impact on consumer rights. Their studies highlight that manipulative digital designs have become a common feature of online platforms and require stronger legal regulation.

Brignull (2010) first introduced the term "Dark Patterns" to describe user interface designs that intentionally mislead or manipulate users into making decisions that benefit businesses rather than consumers. His work laid the foundation for later legal and policy discussions by identifying different forms of deceptive interface designs such as hidden costs, forced continuity and trick questions[3].

The Organisation for Economic Co-operation and Development (OECD) (2022) observed that dark patterns are increasingly used across digital platforms to influence consumer behaviour. The report noted that many consumers are unable to recognise manipulative interface designs, making them vulnerable to financial loss and uninformed decision-making. It emphasised the need for governments to strengthen consumer protection laws in the digital economy[4].

The European Commission (2022) conducted a behavioural study on unfair commercial practices in digital markets. The study concluded that many online consumers unknowingly agreed to purchases, subscriptions or data-sharing practices because websites were intentionally designed to influence their choices. It recommended greater transparency and stricter regulation of deceptive interface designs[5].

In the Indian context, legal scholars have discussed the significance of the CCPA Guidelines on Dark Patterns, 2023 as the country's first dedicated regulatory framework addressing deceptive online practices. While these guidelines have been widely appreciated, many researchers argue that effective implementation will depend on stronger enforcement mechanisms, consumer awareness and regulatory oversight rather than guidelines alone.

Overall, the existing literature agrees that dark patterns undermine informed consumer choice and weaken digital trust. However, there remains limited research examining the practical effectiveness of India's legal framework after the introduction of the 2023 Guidelines. This study attempts to fill that gap by evaluating the present legal

---

[3] Harry Brignull, *Dark Patterns* (2010), available at https://www.deceptive.design/."
[4] Organisation for Economic Co-operation and Development, *Dark Commercial Patterns*, OECD Digital Economy Papers No. 336 (2022).
[5] European Commission, *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation* (2022)

framework, comparing it with international developments and suggesting reforms suitable for the Indian digital marketplace.

IV. UNDERSTANDING DARK PATTERNS IN E-COMMERCE

A. Meaning of Dark Patterns

The term "dark patterns" refers to deceptive or manipulative design techniques used by websites and mobile applications to influence users into making decisions that they may not have made voluntarily. These designs are intentionally created to benefit the business, often at the expense of the consumer. Instead of helping users make informed choices, dark patterns create confusion, pressure or inconvenience, making it easier for businesses to increase sales, collect personal data or retain subscriptions.

The expression "dark patterns" was first introduced by user experience designer Harry Brignull in 2010. Since then, the concept has gained global attention because many digital platforms have started using such practices in online shopping, travel bookings, food delivery applications and subscription-based services.

In India, the Central Consumer Protection Authority (CCPA) officially recognised dark patterns through the *Guidelines for Prevention and Regulation of Dark Patterns, 2023*,[6] making India one of the first countries to specifically identify and prohibit these deceptive digital practices.

B. Characteristics of Dark Patterns

Although dark patterns may appear in different forms, they generally share certain common features.

---

[6] Central Consumer Protection Authority, Advisory No. CCPA-1/1/2023-CCPA, *Advisory in terms of Consumer Protection Act, 2019 on Self-Audit by E-Commerce Platforms for Detecting the Dark Patterns on Their Platforms to Create a Fair, Ethical and Consumer-Centric Digital Ecosystem* dated 5 June 2025; Press Information Bureau, *Central Consumer Protection Authority Issues Advisory to E-Commerce Platforms for Self-Audit within 3 Months to Detect Dark Patterns and Ensure Its Resolution* dated 7 June 2025; Press Information Bureau, *26 Leading E-Commerce Platforms Declare Compliance with Self-Audit to Eliminate Dark Patterns* dated 20 November 2025.

1. They are intentionally designed to influence consumer behaviour.
2. They reduce the consumer's ability to make an informed decision.
3. They prioritise the commercial interests of businesses over consumer welfare.
4. They often hide or delay important information until the final stage of a transaction.
5. They create unnecessary difficulty when consumers try to refuse offers, cancel subscriptions or delete accounts.

Unlike ordinary advertising, which openly promotes products or services, dark patterns operate subtly. Many consumers do not even realise that they have been manipulated until after completing a transaction.

C. Common Types of Dark Patterns

The CCPA Guidelines identify several types of dark patterns that are commonly used in digital platforms. Some of the most frequently observed practices are discussed below:

1. **False Urgency:** False urgency creates an artificial sense of scarcity by displaying messages such as *"Only 1 item left"* or *"Offer ends in 2 minutes."* These messages encourage consumers to make quick decisions without properly comparing products or considering alternatives.
2. **Basket Sneaking:** Basket sneaking occurs when additional products, services or donations are automatically added to a consumer's shopping cart without their clear consent. Unless the consumer carefully reviews the order summary, they may unknowingly pay for unwanted items.
3. **Drip Pricing:** In drip pricing, businesses initially advertise a lower price but gradually add additional charges such as convenience fees, handling charges or service fees during the final stages of payment. As consumers have already invested time in the purchasing process, many proceed with the payment despite the increased cost.

4. **Subscription Traps:** Some online platforms make subscribing to a service simple but intentionally make cancellation lengthy and complicated. Consumers may have to navigate several pages, contact customer support or wait for approval before ending their subscriptions.
5. **Confirm shaming:** Confirm shaming uses emotionally manipulative language to make consumers feel guilty for rejecting an offer. For example, instead of simply asking whether a consumer wishes to decline a subscription, a website may display options such as *"No, I don't want to save money"* or *"No, I don't care about my health."*
6. **Disguised Advertisements:** Some advertisements are designed to resemble genuine search results or recommendations. As a result, consumers may click on promotional content believing it to be independent information.

These practices demonstrate how digital interface design can influence consumer decisions without using direct force or false statements.

D. Impact of Dark Patterns on Consumers

Dark patterns have a significant impact on consumer rights and confidence in digital commerce. Their effects go beyond financial loss and also affect consumer autonomy, privacy and informed consent.

Firstly, consumers may end up purchasing products or services that they never intended to buy. Hidden charges, automatic additions and misleading offers often increase the final cost of transactions.

Secondly, dark patterns reduce consumer choice by creating psychological pressure. Consumers frequently make hurried decisions because they fear losing limited-time offers or discounts.

Thirdly, many dark patterns encourage users to share unnecessary personal information or accept privacy policies without fully understanding their consequences. This raises concerns regarding data protection and informed consent in the digital environment.

 (ISSN: 2583-7753)

Finally, the continued use of deceptive practices reduces public confidence in online marketplaces. Consumers who repeatedly experience misleading transactions may lose trust in digital commerce, affecting both businesses and the overall growth of the digital economy.

E. Need for Legal Regulation

Since dark patterns exploit consumer behaviour rather than providing false information directly, they are often difficult to regulate under traditional consumer protection laws. Existing legal provisions primarily focus on misleading advertisements and unfair trade practices, whereas dark patterns manipulate the consumer through website design and interface architecture.

Therefore, dedicated legal regulation has become necessary to ensure that digital platforms maintain transparency, fairness and accountability. Regulatory authorities must not only prohibit deceptive designs but also create effective enforcement mechanisms that protect consumers from emerging digital practices.

The introduction of the CCPA Guidelines represents an important beginning. However, whether these guidelines alone are sufficient remains an important question, which will be examined in the following chapters.

V. LEGAL FRAMEWORK REGULATING DARK PATTERNS IN INDIA

A. Consumer Protection Act, 2019

The Consumer Protection Act, 2019 is the primary legislation that protects consumer rights in India. Although the Act does not specifically use the term “dark patterns”, many such practices fall within the scope of unfair trade practices and misleading advertisements. The Act aims to ensure that consumers receive accurate information and are not deceived while purchasing goods or services.

Section 2(47)[7] of the Act defines an unfair trade practice as any deceptive or unfair method adopted for promoting the sale or supply of goods and services. Many dark patterns, such as false urgency, drip pricing and hidden charges, can be interpreted as unfair trade practices because they influence consumers through misleading methods rather than allowing them to make informed decisions.

The Act also established the Central Consumer Protection Authority (CCPA) to investigate violations of consumer rights, issue directions against unfair trade practices and impose penalties where necessary.

However, one limitation of the Act is that it was enacted before dark patterns became a significant concern in digital commerce. As a result, it addresses these practices only indirectly and does not contain specific provisions regulating manipulative interface design.

B. Consumer Protection (E-Commerce) Rules, 2020

With the rapid expansion of online marketplaces, the Government introduced the Consumer Protection (E-Commerce) Rules, 2020[8] to regulate digital commerce and strengthen consumer rights.

The Rules require e-commerce entities to provide clear information regarding products, prices, refund policies, delivery charges and grievance redressal mechanisms. They also prohibit unfair trade practices and misleading advertisements by online platforms.

These Rules promote transparency by requiring sellers to disclose important information before consumers complete a purchase. Such requirements reduce the possibility of consumers being misled during online transactions.

Despite these protections, the Rules do not specifically address manipulative website or application designs. For example, while they require accurate disclosure of prices, they

[7] Consumer Protection Act, 2019, No. 35 of 2019, s. 2(47) (India).
[8] Consumer Protection (E-Commerce) Rules, 2020, notified under the Consumer Protection Act, 2019 (India).

 (ISSN: 2583-7753)

do not directly prohibit practices such as repeated pop-up notifications, confusing cancellation procedures or emotional manipulation through interface design. Consequently, many dark patterns continued to exist even after the Rules came into force.

C. CCPA Guidelines for Prevention and Regulation of Dark Patterns, 2023

Recognising the increasing misuse of deceptive online practices, the Central Consumer Protection Authority (CCPA) issued the Guidelines for Prevention and Regulation of Dark Patterns, 2023[9]. These Guidelines represent India's first dedicated regulatory framework specifically addressing dark patterns in digital commerce.

The Guidelines define a dark pattern as any practice or deceptive design that is intended to mislead or manipulate consumers into making choices that they would not have otherwise made. They identify thirteen recognised dark patterns, including:

1. False Urgency
2. Basket Sneaking
3. Confirmshaming
4. Forced Action
5. Subscription Trap
6. Drip Pricing
7. Interface Interference
8. Trick Question
9. Bait and Switch
10. Disguised Advertisement
11. Nagging

[9] Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, Government of India.

12. SaaS Billing

13. Rogue Malwares

By clearly identifying these practices, the Guidelines provide greater certainty to businesses, consumers and enforcement authorities regarding what constitutes unacceptable conduct in digital marketplaces.

The Guidelines also send an important message that digital businesses should compete through transparency and fair practices rather than by manipulating consumer behaviour.

However, these Guidelines are issued under the powers of the Consumer Protection Act and do not create a completely independent legal framework. Their effectiveness therefore depends largely on how actively they are enforced by the regulatory authorities.

D. Digital Personal Data Protection Act, 2023

Dark patterns are not limited to influencing purchases. Many online platforms also use deceptive interface designs to obtain users' personal information or consent for data processing. For instance, users may unknowingly agree to extensive data sharing where the option to refuse consent is hidden, pre-selected, visually de-emphasised or made unnecessarily difficult to exercise.

The Digital Personal Data Protection Act, 2023 seeks to protect individuals by requiring that consent for processing personal data must be free, informed, specific, unambiguous and capable of being signified through clear affirmative action. This standard is particularly relevant to dark patterns because manipulative consent banners, confusing choices and obstructive withdrawal mechanisms may prevent users from making a meaningful and voluntary privacy decision.

The Digital Personal Data Protection Rules, 2025, notified by the Government of India on 14 November 2025, now operationalise this consent framework. The Rules require every Data Fiduciary to provide a separate consent notice that is clear and easy to understand

and that explains the specific purpose for which personal data is collected and processed. These itemised-notice requirements give practical effect to the statutory requirement of informed consent by requiring platforms to communicate data-processing purposes in a manner that ordinary users can understand. In the context of dark patterns, this is significant because deceptive consent interfaces may be challenged where they obscure the purpose of data collection, make refusal difficult, or nudge users into accepting broader processing than they intended.

The Rules also establish a digital-first Data Protection Board of India for complaints, inquiries and enforcement, thereby providing an institutional mechanism for addressing violations of the Act and Rules. Their phased implementation is equally relevant. Certain provisions became effective immediately upon notification, additional obligations relating to consent managers are scheduled to apply after twelve months, and the remaining substantive compliance duties are to come into force after eighteen months. Therefore, although the DPDP Act does not expressly use the term ‘dark patterns’, the Act read with the DPDP Rules, 2025 strengthens the legal basis for challenging manipulative consent designs that undermine free, informed, specific and unambiguous consent.

E. Judicial and Regulatory Developments

“Indian courts have not yet delivered many landmark judgments dealing exclusively with dark patterns. Since the concept has only recently gained express regulatory recognition, judicial interpretation is still evolving. Nevertheless, courts have consistently recognised that consumers are entitled to truthful information and protection against deceptive commercial practices. These principles are likely to guide future adjudication involving manipulative digital interfaces.

Regulatory developments in 2025 indicate a shift from general recognition of dark patterns towards active compliance monitoring. On 5 June 2025, the Central Consumer Protection Authority issued Advisory No. CCPA-1/1/2023-CCPA under the Consumer Protection Act, 2019, directing e-commerce platforms and online service providers to conduct self-audits to detect and eliminate dark patterns. The advisory, effective from 6 June 2025 to 31 December 2026, required platforms to identify deceptive design practices, take corrective measures and submit self-declarations confirming that their platforms do not indulge in dark patterns. The Press Information Bureau's release dated 7 June 2025 further records that platforms were advised to complete such self-audits within three months and ensure compliance with the Guidelines for Prevention and Regulation of Dark Patterns, 2023.

The CCPA has also taken concrete enforcement steps against specific practices. A notable example is the BookMyShow matter, where the platform was found to be automatically adding a pre-ticked ₹1 contribution towards its 'BookASmile' initiative during ticket booking. This practice was treated as 'Basket Sneaking' under Annexure I of the 2023 Guidelines because an additional payment was added without the consumer's express consent. After the CCPA's intervention, BookMyShow modified the interface by allowing consumers to choose whether or not they wished to contribute.

These developments strengthen the empirical basis for assessing India's enforcement framework. They show that the CCPA is no longer confined to issuing general policy guidance, but is also using advisories, notices, self-audits and self-declarations to secure platform-level compliance. At the same time, the self-audit model has limitations. Unless self-declarations are supported by independent verification, public transparency and follow-up action against non-compliant platforms, deceptive interface practices may continue despite formal compliance claims. Therefore, while the 2025 advisory and BookMyShow action represent important progress, continuous regulatory monitoring remains necessary to ensure that dark-pattern regulation is effective in practice."

F. Critical Analysis of the Present Framework

India has undoubtedly taken an important step by officially recognising dark patterns and introducing dedicated guidelines. This demonstrates the government's intention to create a safer digital marketplace.

 (ISSN: 2583-7753)

However, certain limitations continue to exist.

First, there is no separate legislation exclusively dealing with dark patterns. Most enforcement still depends on the broader provisions of the Consumer Protection Act.

Secondly, identifying and proving the existence of a dark pattern is often difficult. Businesses may argue that certain interface designs merely improve user experience rather than manipulate consumer choices.

Another challenge is the lack of consumer awareness. Many individuals are unaware that they have been influenced by deceptive digital designs and therefore do not report such practices.

Finally, regulatory authorities face practical difficulties in monitoring thousands of websites, mobile applications and online marketplaces operating across the country.

For these reasons, while India's legal framework has made significant progress, stronger enforcement mechanisms and continuous regulatory supervision remain essential.

VI. COMPARATIVE ANALYSIS: INTERNATIONAL APPROACHES TO REGULATING DARK PATTERNS

The increasing use of dark patterns is not limited to India. Many countries have recognised that deceptive digital practices affect consumer rights and have introduced legal measures to regulate them. Examining these international approaches helps in understanding how India can strengthen its own regulatory framework.

A. European Union (EU)

The European Union has adopted one of the most comprehensive approaches to regulating dark patterns. Through the Digital Services Act (DSA), online platforms are prohibited from designing interfaces that deceive, manipulate or materially distort users' ability to make free and informed decisions. The DSA therefore directly addresses manipulative interface design as part of the wider regulation of online platforms. The DSA places greater responsibility on large online platforms to ensure that their digital services are transparent and fair. It discourages deceptive consent requests, misleading subscription options and manipulative interface designs. The legislation also requires major platforms to assess systemic risks created by their services and take steps to minimise consumer harm. One of the strengths of the European model is its strict enforcement mechanism, including the possibility of significant financial penalties for non-compliance.

At the same time, recent EU policy developments show that even the DSA is not regarded as a complete answer to dark patterns. Following the Digital Fairness Fitness Check of EU consumer law, published in October 2024, the European Commission indicated that it was preparing a Digital Fairness Act to address remaining gaps in the digital consumer protection framework. The proposed initiative is expected to target harmful practices such as dark patterns, manipulative interface design, misleading influencer marketing, addictive digital design and unfair personalisation. This forward-looking development is significant for India because it shows that even jurisdictions with advanced digital regulation continue to strengthen their legal frameworks as new forms of online manipulation emerge.

B. United States

Unlike the European Union, the United States does not have a single federal statute dealing exclusively with dark patterns. Instead, the regulation of such practices is generally pursued through existing consumer protection laws prohibiting unfair or deceptive acts or practices, including laws relating to online subscriptions and negative-option marketing.

The Federal Trade Commission has played an active role in challenging manipulative digital interfaces, particularly where platforms use misleading enrolment processes, obstruct cancellation, or obtain consumer consent through deceptive design. A significant example is *Federal Trade Commission v. Amazon.com, Inc.*, where the FTC alleged that Amazon used manipulative, coercive and deceptive user-interface designs to enrol consumers in automatically renewing Prime subscriptions and made cancellation

 (ISSN: 2583-7753)

unnecessarily difficult. Although the case was initially filed in 2023, it is no longer merely pending litigation. On 25 September 2025, the FTC and Amazon entered into a landmark settlement of $2.5 billion, comprising a $1 billion civil penalty and $1.5 billion in consumer redress. The settlement also imposed structural conduct requirements, including a clear option to decline Prime, clear disclosure of material subscription terms during enrolment, and a simpler cancellation mechanism.

This settlement strengthens the comparative relevance of the United States model. It demonstrates that, even in the absence of a dedicated dark-patterns statute, active enforcement under general consumer protection law can produce substantial monetary penalties as well as mandatory redesign of manipulative enrolment and cancellation flows. For India, the case illustrates the importance of combining regulatory recognition of dark patterns with meaningful penalties, corrective directions and continuing supervision of digital platforms.

C. United Kingdom

The United Kingdom has also strengthened consumer protection in digital markets through the Digital Markets, Competition and Consumers Act, 2024. The Act enhances the Competition and Markets Authority's consumer enforcement powers and updates the legal framework on unfair commercial practices, subscription contracts and online consumer transactions. Its core consumer-protection and enforcement provisions came into force on 6 April 2025, while the subscription-contract reforms have been deferred and are not expected to commence before spring 2026.

The UK approach is therefore important, but it should not be overstated as a comprehensive dark-patterns regime. The Act targets several practices that commonly overlap with dark patterns, including fake reviews, drip pricing, subscription traps and unclear online purchasing processes. However, specialist commentary has noted that the Act makes only limited changes in respect of online choice architecture or dark patterns as a distinct regulatory category. It does not create a general prohibition on manipulative interface design comparable in form to India's CCPA Guidelines on Dark Patterns, 2023.

 (ISSN: 2583-7753)

Compared to India, the United Kingdom provides stronger statutory enforcement powers and a more developed penalty framework. However, its dark-pattern-relevant provisions remain targeted at specific harmful practices rather than framed as a broad catalogue of prohibited interface designs. This distinction is significant for comparative analysis, as it shows that jurisdictions may regulate dark patterns either through a general design-focused framework, as India has attempted through guidelines, or through practice-specific consumer-protection rules, as reflected in the United Kingdom's current approach.

D. India

The comparative study shows that India has made important progress by officially recognising dark patterns through the CCPA Guidelines. However, countries such as the European Union and the United Kingdom have moved beyond merely identifying deceptive practices by introducing stronger enforcement mechanisms and imposing stricter penalties for violations.

India can learn several important lessons from these jurisdictions.

Firstly, enforcement should be strengthened by providing regulators with greater investigative and monitoring powers.

Secondly, penalties should be sufficiently stringent to discourage businesses from adopting deceptive digital practices merely for commercial gain.

Thirdly, digital platforms should be encouraged to follow ethical design principles from the initial stage of developing websites and mobile applications rather than correcting problems only after complaints are received.

Finally, consumer awareness programmes should be expanded so that individuals can recognise dark patterns and exercise their rights more effectively.

 (ISSN: 2583-7753)

Overall, while India's legal framework has established a good foundation, international experience demonstrates that effective implementation and continuous regulatory oversight are equally important for protecting consumers in the digital economy.

VII. CHALLENGES IN REGULATING DARK PATTERNS AND THE WAY FORWARD

Although India has introduced specific guidelines to regulate dark patterns, several practical challenges continue to affect their implementation.

A. Lack of Consumer Awareness

Many consumers are unfamiliar with the concept of dark patterns. They often believe that hidden charges, misleading offers or complicated cancellation procedures are normal features of online shopping. As a result, only a small number of affected consumers file complaints before the appropriate authorities.

Consumer awareness campaigns, digital literacy programmes and educational initiatives are therefore essential to help individuals recognise deceptive online practices and make informed decisions.

B. Rapid Technological Developments

Technology evolves much faster than legislation. Digital businesses continuously introduce new interface designs and marketing strategies that may not be covered by existing regulations.

This makes it difficult for regulators to identify emerging forms of manipulation and update legal frameworks quickly enough to address new challenges.

C. Enforcement Challenges

Enforcing regulations against dark patterns is often more difficult than identifying them. Many online platforms operate across different countries and frequently modify their websites or mobile applications. Regulators therefore require technical expertise and continuous monitoring to detect violations effectively.

 (ISSN: 2583-7753)

Moreover, proving that a particular interface was intentionally designed to manipulate consumers may require detailed technical examination, making investigations both time-consuming and resource-intensive.

D. Constitutional Perspective

Dark patterns are not merely a consumer protection issue; they also raise important constitutional concerns. When digital platforms obtain consent through deceptive designs or pressure users into sharing personal information, the principles of privacy, autonomy and informed consent may be affected.

The Supreme Court, in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017),[10] recognised privacy as a fundamental right under Article 21 of the Constitution. This judgment highlights that consent should be meaningful and voluntary rather than obtained through manipulation or deception.

Therefore, regulating dark patterns is also important from the perspective of protecting individual dignity and personal autonomy in the digital age.

VIII. SUGGESTIONS AND RECOMMENDATIONS

1. Strengthen the Legal Framework

Although the CCPA Guidelines, 2023 specifically identify and prohibit dark patterns, they function as guidelines under the Consumer Protection Act, 2019. A separate statutory provision or suitable amendments to the Consumer Protection Act may provide greater legal certainty and stronger enforcement against deceptive digital practices.

2. Enhance Regulatory Enforcement

The Central Consumer Protection Authority should be provided with adequate technical resources and trained personnel to monitor digital platforms regularly. Proactive monitoring can help identify violations before they affect a large number of consumers.

---

[10] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

 (ISSN: 2583-7753)

3. **Increase Consumer Awareness**

Many consumers are unaware of manipulative online practices and often become victims without realising it. Public awareness campaigns, educational programmes and digital literacy initiatives should be conducted to educate consumers about dark patterns and their legal rights.

4. **Encourage Ethical Interface Design**

E-commerce platforms should adopt transparent and consumer-friendly interface designs. Businesses should ensure that pricing, cancellation procedures, subscriptions and consent requests are presented clearly without misleading or pressuring consumers.

5. **Promote Industry Self-Regulation**

Apart from legal enforcement, industry bodies and digital businesses should voluntarily adopt ethical standards and best practices. Regular compliance audits and transparent business policies can improve consumer confidence in digital marketplaces.

6. **Strengthen Inter-Agency Coordination**

Since dark patterns may involve consumer protection, data privacy and digital commerce, greater coordination between the Central Consumer Protection Authority (CCPA), the Ministry of Consumer Affairs and other relevant regulatory bodies would improve enforcement and policy implementation.

IX. CONCLUSION

The rapid growth of e-commerce has transformed India's digital economy by making goods and services more accessible to consumers. However, this technological progress has also resulted in the increasing use of dark patterns, which manipulate consumer behaviour through deceptive interface designs rather than through direct misrepresentation.

India has taken a significant step by introducing the Guidelines for Prevention and Regulation of Dark Patterns, 2023, making it one of the few countries to specifically

 (ISSN: 2583-7753)

recognise and regulate such practices. Along with the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020, these guidelines provide an important legal foundation for safeguarding consumer interests in the digital marketplace.

Despite these developments, several challenges continue to exist. The present framework largely depends on general consumer protection provisions, while technological innovations continue to create new forms of digital manipulation. Limited consumer awareness, practical enforcement difficulties and the absence of a dedicated statutory framework further reduce the effectiveness of existing regulations.

The comparative study of the European Union, the United States and the United Kingdom demonstrates that effective consumer protection requires not only clear legal rules but also strong regulatory oversight, timely enforcement and continuous monitoring of digital platforms.

In conclusion, protecting consumers in the digital age requires a balanced approach that promotes technological innovation while ensuring fairness, transparency and informed consumer choice. Strengthening legal enforcement, encouraging ethical digital practices and improving consumer awareness will play a vital role in building a safer and more trustworthy digital marketplace in India.

X. REFERENCES

1. Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, Government of India

2. Consumer Protection Act, 2019, No. 35 of 2019 (India).

3. Consumer Protection (E-Commerce) Rules, 2020, notified under the Consumer Protection Act, 2019 (India).

4. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

5. Ministry of Electronics and Information Technology, *Digital Personal Data Protection Rules, 2025*, Government of India.
6. Ministry of Electronics and Information Technology. (2025, November 14). *Government notifies DPDP Rules to empower citizens and protect privacy*. Government of India.
7. Harry Brignull, *Dark Patterns* (2010), available at https://www.deceptive.design/."
8. European Commission, *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation* (2022).
9. Organisation for Economic Co-operation and Development, *Dark Commercial Patterns*, OECD Digital Economy Papers No. 336 (2022).
10. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC [Digital Services Act], art. 25; European Commission, *Digital Fairness Act* initiative, following the Digital Fairness Fitness Check of EU consumer law published on 3 October 2024.
11. Digital Markets, Competition and Consumers Act 2024, c. 13 (UK); Digital Markets, Competition and Consumers Act 2024 (Commencement No. 2 and Transitional Provisions) Regulations 2025; UK Parliament, Written Answer to Question 24132, 22 January 2025, noting commencement of consumer enforcement and unfair-commercial-practices reforms in April 2025 and subscription-contract reforms not before spring 2026.
12. *Federal Trade Commission v. Amazon.com, Inc.*, No. 2:23-cv-00932-JHC (W.D. Wash. filed 21 June 2023); Federal Trade Commission, *FTC Secures Historic $2.5 Billion Settlement Against Amazon* (25 September 2025).
13. Federal Trade Commission, *FTC Secures Historic $2.5 Billion Settlement Against Amazon* (25 September 2025).

14. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

15. Digital Markets, Competition and Consumers Act 2024 (Commencement No. 2 and Transitional Provisions) Regulations 2025 (UK).

16. UK Parliament, Written Answer to Question 24132, 22 January 2025.

17. Lewis Silkin, *Our Guide to the Digital Markets, Competition and Consumers Act 2024 – Focusing on Consumer Law*.

 (ISSN: 2583-7753)