

Dark Patterns as Digital Consumer Abuse: Towards Criminalization under Indian Consumer Law

Rajat Umrey¹

¹Assistant Professor, Department of MBA, Lakshmi Narain College of Technology University, Bhopal (M.P.), India

Abstract

The rapid expansion of digital commerce has transformed consumer transactions while simultaneously facilitating deceptive interface designs known as **dark patterns**, which manipulate consumer behaviour and undermine informed decision-making. Although India has introduced the **Consumer Protection Act, 2019**, the **Consumer Protection (E-Commerce) Rules, 2020**, and the **Guidelines for Prevention and Regulation of Dark Patterns, 2023**, the existing legal framework primarily relies on civil and regulatory remedies. Consequently, questions remain regarding the adequacy of these measures in addressing deliberate and repeated digital consumer abuse. This study examines whether aggravated forms of dark patterns should attract criminal liability under Indian consumer law. Using a doctrinal legal research methodology supported by comparative analysis of legal frameworks in the European Union, the United States, and the United Kingdom, the paper evaluates the effectiveness of the current Indian regulatory regime. The study finds that while ordinary instances of dark patterns may be adequately addressed through civil enforcement, intentional, repeated, and financially harmful manipulative practices justify selective criminalization. The paper contributes to the emerging discourse on digital consumer protection by proposing a balanced legal framework that strengthens deterrence, enhances consumer confidence, and promotes accountability without impeding technological innovation.

Keywords: Dark patterns, digital consumer protection, consumer law, criminal liability, deceptive design, e-commerce, consumer rights, digital governance.

1. Introduction

The rapid digitalization of commerce has fundamentally transformed the manner in which consumers purchase goods and services. Online marketplaces, mobile applications, digital payment systems, and subscription-based platforms have significantly enhanced convenience, accessibility, and market efficiency. However, alongside these developments, businesses have increasingly adopted sophisticated interface designs that influence consumer behaviour through psychological manipulation rather than informed choice. These deceptive interface techniques, commonly referred to as **dark patterns**, exploit cognitive biases to encourage consumers to make decisions that primarily benefit digital service providers. Common examples include hidden charges, misleading countdown timers, forced subscriptions, disguised advertisements, privacy manipulation, and complicated cancellation procedures.

The growing dependence on digital platforms in India has considerably increased consumer exposure to such manipulative practices. Recognizing these concerns, the Government of India introduced the **Guidelines for**

Prevention and Regulation of Dark Patterns, 2023, supplementing the **Consumer Protection Act, 2019** and the **Consumer Protection (E-Commerce) Rules, 2020**. These legal instruments prohibit several deceptive online practices and strengthen consumer protection in the digital marketplace. Nevertheless, enforcement continues to rely predominantly on administrative directions, regulatory penalties, and consumer dispute resolution mechanisms. The absence of explicit criminal liability raises important questions regarding the effectiveness of existing legal remedies in addressing intentional and repeated digital manipulation.

Existing scholarship primarily focuses on identifying dark patterns, analysing consumer behaviour, and evaluating regulatory compliance. Comparatively little attention has been devoted to examining whether severe forms of digital consumer manipulation should attract criminal sanctions under Indian consumer law. This represents a significant research gap, particularly in light of increasing algorithmic personalization, behavioural targeting, and large-scale digital commerce.

Accordingly, this study seeks to evaluate the adequacy of India's existing legal framework governing dark patterns and to assess the legal justification for introducing selective criminal liability in cases involving fraudulent intent, repeated misconduct, or substantial consumer harm. Through comparative analysis of international regulatory approaches, the paper proposes a balanced legal framework that protects consumer autonomy while preserving technological innovation and legitimate commercial practices. The findings are expected to contribute to the ongoing development of digital consumer protection policy in India.

2. Literature Review

The concept of dark patterns has attracted increasing scholarly attention as digital commerce has expanded globally. Gray et al. (2018) defined dark patterns as deceptive interface designs intentionally created to manipulate consumer decisions by exploiting behavioural and cognitive biases. Their classification has become the foundation for subsequent legal and technological research. Similarly, Mathur et al. (2019) demonstrated the widespread use of dark patterns across commercial websites, revealing that deceptive interface designs often produce substantial economic benefits for businesses while reducing consumer autonomy and informed consent.

Behavioural economics provides the theoretical basis for understanding these practices. Thaler and Sunstein (2008) argued that consumer decisions are frequently influenced by cognitive heuristics, default settings, framing effects, and decision fatigue. Digital platforms increasingly utilize these behavioural principles to encourage purchases, subscriptions, or disclosure of personal information. Consequently, recent legal scholarship has recognized dark patterns as a distinct category of unfair commercial practice requiring specialized

regulatory intervention beyond traditional consumer protection laws.

Within the Indian context, researchers have examined the role of the **Consumer Protection Act, 2019**, the **Consumer Protection (E-Commerce) Rules, 2020**, and the **Guidelines for Prevention and Regulation of Dark Patterns, 2023** in strengthening digital consumer rights. Although these legal measures represent significant regulatory progress, existing studies consistently identify limitations relating to enforcement capacity, technological complexity, jurisdictional challenges, and the absence of explicit criminal sanctions for deliberate and repeated violations.

Despite growing international literature on digital consumer protection, limited research has critically examined the normative and legal justification for criminalizing aggravated forms of dark patterns under Indian consumer law. Most available studies emphasize regulatory compliance and administrative enforcement while overlooking the potential role of criminal law in deterring intentional digital consumer abuse. By addressing this gap, the present study contributes to legal scholarship by evaluating whether selective criminalization can provide a proportionate and effective response to serious forms of deceptive digital practices without discouraging innovation or legitimate business activities.

3. Materials and Methods

This study adopts a **qualitative doctrinal legal research design** to examine whether dark patterns constitute a form of digital consumer abuse warranting selective criminalization under Indian consumer law. Doctrinal legal research is appropriate for this study because it facilitates a systematic examination of statutory provisions, judicial precedents, regulatory guidelines, constitutional principles, and scholarly literature to evaluate the adequacy of the existing legal framework governing deceptive digital practices. Unlike empirical studies that rely on surveys or interviews, doctrinal research focuses on analysing legal rules, interpreting legislative intent, and assessing the effectiveness of legal mechanisms in addressing contemporary regulatory challenges. The study is guided by three objectives:

- (i) to analyse the existing legal framework governing dark patterns in India,
- (ii) to compare India's regulatory approach with selected international jurisdictions, and
- (iii) to evaluate whether aggravated forms of dark patterns justify selective criminalization under Indian consumer law. These objectives provide the analytical framework for examining the strengths and limitations of the current regulatory regime.

The research relies exclusively on **secondary sources**. Primary legal materials include the **Consumer Protection Act, 2019**, the **Consumer Protection (E-Commerce) Rules, 2020**, the **Guidelines for Prevention and Regulation of Dark Patterns, 2023**, the **Digital Personal Data Protection Act, 2023**, relevant constitutional provisions, judicial decisions, and official government notifications. Secondary sources comprise peer-reviewed journal articles, legal commentaries, books, reports published by government agencies, Law Commission reports, international policy documents, and publications issued by regulatory authorities. Only authentic and authoritative legal databases and official government sources were considered to ensure the reliability and credibility of the analysis.

A **comparative legal approach** was adopted to examine regulatory developments in the **European Union, the United States, and the United Kingdom**. These jurisdictions were selected because they have developed relatively advanced legal and regulatory mechanisms addressing deceptive online commercial practices. The comparative analysis focused on statutory definitions of dark patterns, enforcement mechanisms, regulatory penalties, judicial interpretations, and circumstances in which criminal liability may arise. Comparative legal analysis enabled the identification of international best practices and facilitated the formulation of recommendations suitable for the Indian legal system.

The collected legal materials were analysed using **thematic content analysis**. The analysis was organized around five principal themes: (i) conceptual understanding of dark patterns, (ii) existing legal and regulatory mechanisms in India, (iii) enforcement challenges and regulatory gaps, (iv) comparative legal approaches, and (v) legal justification for selective criminalization. Relevant statutory provisions, judicial observations, regulatory guidelines, and academic opinions were systematically examined and categorized under these themes to identify recurring legal principles, inconsistencies, and policy deficiencies.

To enhance the reliability of the findings, **methodological triangulation** was employed by comparing statutory provisions, judicial precedents, government guidelines, regulatory reports, and contemporary academic literature. This cross-verification minimized interpretative bias and strengthened the validity of the legal analysis. Since the study relied exclusively on publicly available legal documents and published literature, **ethical approval was not required**.

The study has certain limitations. As a doctrinal legal study, it does not include empirical evidence regarding consumer perceptions or the prevalence of dark patterns in digital marketplaces. Moreover, because India's regulatory framework concerning dark patterns is relatively recent, judicial precedents and enforcement data remain limited. Nevertheless, the adopted methodology provides an appropriate basis for evaluating the adequacy of the current legal framework and proposing policy recommendations regarding the selective criminalization of serious forms of digital consumer abuse.

Table 1. Research Design

Component	Description
Research approach	Qualitative doctrinal legal research
Research design	Analytical and comparative legal study
Research objectives	Analyse the Indian legal framework; compare international approaches; evaluate criminalization
Nature of data	Secondary legal and academic sources
Primary legal sources	Consumer Protection Act, 2019; Consumer Protection (E-Commerce) Rules, 2020; Guidelines for Prevention and Regulation of Dark Patterns, 2023; Digital Personal Data Protection Act, 2023; constitutional provisions; judicial decisions
Secondary sources	Peer-reviewed journals, books, legal commentaries, government reports, Law Commission reports, international publications
Comparative jurisdictions	India, European Union, United States, United Kingdom

Analytical technique	Thematic content analysis with doctrinal interpretation
Reliability measure	Triangulation of statutes, case law, regulatory documents, and scholarly literature
Outcome	Assessment of legal adequacy and proposal for selective criminalization

Table 2. Legal Sources Reviewed

Legal Instrument	Jurisdiction	Purpose in the Study
Consumer Protection Act, 2019	India	Consumer rights, unfair trade practices, regulatory framework
Consumer Protection (E-Commerce) Rules, 2020	India	Regulation of e-commerce platforms and consumer protection
Guidelines for Prevention and Regulation of Dark Patterns, 2023	India	Identification and prohibition of deceptive interface designs
Digital Personal Data Protection Act, 2023	India	Protection of personal data and informed digital consent
Constitution of India	India	Consumer welfare, equality, and reasonable restrictions
Digital Services Act	European Union	Platform accountability and online consumer protection
Unfair Commercial Practices Directive	European Union	Regulation of deceptive commercial practices
Federal Trade Commission Act (Section 5)	United States	Regulation of unfair and deceptive business practices
Consumer Protection from Unfair Trading Regulations	United Kingdom	Prevention of misleading commercial practices



Figure 1. Research Methodology

4. Results and Discussion

The doctrinal and comparative legal analyses reveal that India's regulatory framework has made significant progress in addressing deceptive digital practices. However, important legal and institutional gaps continue to limit the effectiveness of consumer protection against dark patterns. The findings are discussed under five thematic categories.

4.1 Recognition of Dark Patterns under Indian Consumer Law

The first finding demonstrates that India has formally recognized **dark patterns** as a distinct category of unfair digital commercial practice. The issuance of the **Guidelines for Prevention and Regulation of Dark Patterns, 2023** represents a significant regulatory milestone because it explicitly identifies deceptive interface designs that manipulate consumer decision-making. These guidelines complement the **Consumer Protection Act, 2019** and the **Consumer Protection (E-Commerce) Rules, 2020** by extending the concept of unfair trade practices to digital commerce.

The analysis indicates that online platforms are now legally expected to ensure transparency in pricing, subscription models, advertising practices, consent mechanisms, cancellation procedures, and data collection practices. This regulatory development reflects India's commitment to strengthening digital consumer rights in response to the rapid expansion of e-commerce and online service platforms.

4.2 Limitations of the Existing Enforcement Framework

Despite the existence of a comprehensive regulatory framework, the study identifies significant enforcement limitations. The current legal regime primarily relies on **administrative directions, monetary penalties, and consumer dispute resolution mechanisms**. The Central Consumer Protection Authority (CCPA) possesses investigative and enforcement powers; however, intentional deployment of deceptive interface designs generally attracts

civil or administrative consequences rather than criminal liability.

The findings indicate that this approach may be inadequate where businesses deliberately employ behavioural manipulation, algorithmic personalization, hidden subscription models, or misleading interface architecture to obtain unlawful economic benefits. For large digital platforms, regulatory penalties may represent ordinary operational expenses rather than effective deterrents. Consequently, repeated violations may continue despite existing regulatory interventions.

4.3 Comparative Analysis of International Legal Frameworks

Comparative legal analysis demonstrates that the **European Union**, **United States**, and **United Kingdom** have progressively strengthened regulatory oversight of deceptive online commercial practices. Although these jurisdictions also rely primarily on administrative enforcement, they provide stronger investigative powers, higher financial penalties, stricter compliance obligations, and greater regulatory accountability.

The European Union has adopted comprehensive digital governance measures emphasizing transparency, platform accountability, and consumer autonomy. Similarly, the United States regulates deceptive commercial practices through the Federal Trade Commission, while the United Kingdom addresses misleading commercial conduct through dedicated consumer protection legislation. Although criminal liability is generally reserved for aggravated circumstances involving fraud or intentional deception, international developments clearly indicate a shift toward stronger legal responses against manipulative digital practices.

These comparative findings suggest that India may benefit from adopting a graduated enforcement model combining administrative regulation with selective criminal sanctions for the most serious violations.

4.4 Integration of Consumer Protection and Data Governance

Another important finding concerns the increasing convergence between consumer protection and digital data governance. Contemporary dark patterns frequently rely upon behavioural analytics, algorithmic profiling, artificial intelligence, and extensive personal data collection to influence purchasing behaviour. Consequently, deceptive interface design extends beyond misleading visual presentation and increasingly affects **privacy, informed consent, consumer autonomy, and algorithmic accountability**.

The study therefore argues that effective regulation cannot be achieved through consumer protection legislation alone. Rather, enforcement requires coordinated implementation of the **Consumer Protection Act, 2019**, the **Digital Personal Data Protection Act, 2023**, and sector-specific digital governance regulations. Such integration would provide stronger protection against emerging forms of technology-enabled consumer manipulation.

4.5 Legal Justification for Selective Criminalization

The principal finding of this study concerns the legal justification for introducing **selective criminal liability**. The analysis demonstrates that not every dark pattern possesses the same degree of legal culpability. Certain practices involve poor interface design or inadequate disclosure and may be appropriately addressed through regulatory compliance measures. However, aggravated forms involving fraudulent

intent, repeated violations, significant financial harm, or deliberate exploitation of vulnerable consumers require stronger legal intervention.

The principle of proportionality suggests that criminal sanctions should remain an exceptional remedy applicable only where civil and administrative mechanisms fail to provide adequate deterrence. Accordingly, criminal liability should be restricted to situations involving:

- deliberate consumer deception;
- repeated regulatory violations;
- substantial financial or economic loss;
- fraudulent concealment of material information;
- exploitation of children, elderly persons, or digitally vulnerable consumers; and
- large-scale commercial misconduct causing widespread consumer harm.

Such a differentiated approach would preserve legal certainty while ensuring proportionate punishment for serious digital consumer abuse.

4.6 Policy Implications

The findings have important implications for digital consumer governance in India. First, legislative amendments should clearly distinguish between ordinary regulatory violations and aggravated deceptive practices deserving criminal sanctions. Second, enforcement agencies require enhanced digital forensic capacity, algorithmic auditing mechanisms, and specialised technical expertise to investigate sophisticated interface manipulation.

The study further recommends greater institutional coordination among the **Central Consumer Protection Authority (CCPA)**, data protection authorities, competition regulators, cybersecurity agencies, and judicial institutions. Digital platforms should also adopt **privacy-by-design**, transparent interface design, periodic compliance audits, algorithmic accountability, and ethical governance mechanisms to reduce regulatory risks and enhance consumer trust.

Overall, the findings indicate that selective criminalization, supported by effective institutional capacity and corporate compliance, offers the most balanced approach to regulating serious forms of digital consumer abuse while preserving technological innovation and market competitiveness.

Table 3. Classification of Dark Patterns and Suggested Legal Response

Category	Typical Practice	Consumer Impact	Current Legal Position	Recommended Response
False Urgency	Fake countdown timers	Impulsive purchasing	Regulatory violation	Administrative penalty
Hidden Costs	Undisclosed checkout charges	Financial loss	Unfair trade practice	Compensation + monetary penalty
Subscription Trap	Difficult cancellation	Continuous financial loss	Civil remedy	Criminal liability for repeated intentional conduct
Confirm Shaming	Manipulative consent	Impaired consumer	Regulatory action	Compliance direction

	requests	autonomy		
Privacy Manipulation	Misleading consent architecture	Privacy infringement	Data protection violation	Joint consumer-data enforcement
Disguised Advertisement	Sponsored content presented as neutral	Consumer deception	Regulatory penalty	Enhanced monetary penalty
Forced Action	Mandatory registration or permissions	Restricted consumer choice	Administrative action	Consumer compensation
Fraudulent Interface Manipulation	Deliberate deceptive design causing substantial financial harm	Serious digital consumer abuse	Limited legal remedy	Selective criminal prosecution

Table 4. Comparative Legal Framework

Jurisdiction	Principal Legal Instrument	Primary Enforcement	Criminal Liability	Key Learning for India
India	Consumer Protection Act, 2019; Dark Patterns Guidelines, 2023	Administrative and civil	Limited	Strengthen deterrence through selective criminalization
European Union	Digital Services Act; Unfair Commercial Practices Directive	Administrative enforcement	Limited under Member State laws	Strong transparency and platform accountability
United States	Federal Trade Commission Act	FTC investigations and civil enforcement	Available in fraud-related cases	Strong investigative powers
United Kingdom	Consumer Protection from Unfair Trading Regulations	Civil and regulatory enforcement	Available for serious deceptive conduct	Effective regulatory compliance mechanisms

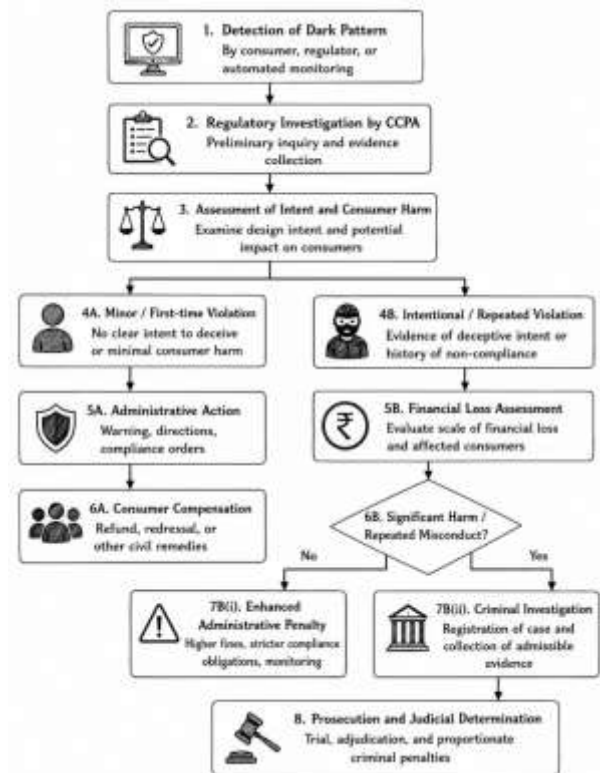


Figure 2. Proposed Regulatory Framework for Selective Criminalization

5. Conclusion

The rapid expansion of digital commerce has significantly increased the prevalence of dark patterns, posing serious challenges to consumer autonomy, informed consent, and fair market practices. This study examined the adequacy of the existing Indian legal framework in regulating deceptive digital interface designs and evaluated the need for selective criminalization of aggravated forms of digital consumer abuse. The doctrinal and comparative analyses indicate that the **Consumer Protection Act, 2019**, the **Consumer Protection (E-Commerce) Rules, 2020**, and the **Guidelines for Prevention and Regulation of Dark Patterns, 2023** have substantially strengthened consumer protection by recognizing and regulating deceptive online practices. Nevertheless, the current enforcement framework remains predominantly civil and administrative, which may not provide adequate deterrence against intentional, repeated, and financially harmful misconduct by digital platforms.

The study concludes that criminal liability should not extend to every instance of dark patterns but should be confined to aggravated cases involving fraudulent intent, repeated violations, substantial consumer harm, or deliberate exploitation of vulnerable consumers. Such a proportionate regulatory approach would enhance legal certainty, strengthen consumer confidence, promote ethical digital commerce, and improve regulatory accountability without discouraging technological innovation. The study also contributes to the emerging discourse on digital consumer protection by proposing a balanced legal framework integrating consumer protection, data governance, and criminal accountability. Future research may complement this doctrinal analysis through empirical studies examining consumer awareness, enforcement practices, and the effectiveness of regulatory interventions in addressing deceptive digital practices.

6. References

1. European Parliament and Council. (2005). *Directive 2005/29/EC concerning unfair business-to-consumer commercial practices*. <https://eur-lex.europa.eu>
2. European Parliament and Council. (2022). *Digital Services Act (Regulation (EU) 2022/2065)*. <https://eur-lex.europa.eu>
3. Government of India. (2019). *The Consumer Protection Act, 2019* (Act No. 35 of 2019). Ministry of Law and Justice.
4. Government of India. (2020). *Consumer Protection (E-Commerce) Rules, 2020*. Ministry of Consumer Affairs, Food and Public Distribution.
5. Government of India. (2023). *Guidelines for Prevention and Regulation of Dark Patterns*. Department of Consumer Affairs.
6. Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Law and Justice.
7. Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. *Proceedings of the ACM Conference on Human Factors in Computing Systems*, 1–14.
8. Luguri, J., & Strahilevitz, L. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43–109.
9. Mathur, A., Acar, G., Friedman, M., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11,000 shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–32.
10. Mathur, A., Narayanan, A., & Chetty, M. (2021). Endorsements on social media: An empirical study of deceptive interface practices. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW), 1–29.
11. Organisation for Economic Co-operation and Development. (2022). *Dark commercial patterns*. OECD Publishing.
12. Sunstein, C. R. (2022). *Sludge: What stops us from getting things done and what to do about it*. MIT Press.
13. Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.
14. United Kingdom Government. (2008). *Consumer Protection from Unfair Trading Regulations 2008*. <https://www.legislation.gov.uk>
15. United States Federal Trade Commission. (1914). *Federal Trade Commission Act* (15 U.S.C. §§ 41–58).
16. United States Federal Trade Commission. (2022). *Bringing dark patterns to light*. Federal Trade Commission Staff Report.
17. World Economic Forum. (2023). *The future of trust in the digital economy*. World Economic Forum.