



DESIGNED TO DECEIVE: RETHINKING CONSUMER CONSENT IN INDIA'S E-COMMERCE ERA

Pulkita Ojha*

ABSTRACT

India's digital market has shown a gradual growth that regulatory measures have struggled to keep up with. Beneath the convenience of one-click shopping and pre-designed tailored feeds are design strategies that quietly limit consumers' choices. This article explores how dark patterns –deceptive user interface techniques have weakened meaningful consent in digital transactions. India's existing consumer protection frameworks include regulations under the Consumer Protection Act 2019, the E-commerce Rules 2020, and the CCPA's guidelines for prevention and regulation of dark patterns 2023, alongside the Digital Personal Data Protection Act 2023. Although the contemporary legal framework is promising, it remains inadequate to address the growing structural problem of interface manipulation. The article centres around the architecture of digital consent and calls for a stronger enforcement regime and a statutory definition of informed consent calibrated to the realities of digital commerce.

Keywords: Dark patterns, consumer consent, e-commerce regulation, Consumer Protection Act 2019, digital manipulation, India.

INTRODUCTION

“Imagine you open Amazon or any online shopping platform. At checkout, you see an extra item in your cart. You did not choose this; the platform chose it for you.” Does that amount to free consent? Consumer protection is based on the idea that a transaction is valid only when the consumer freely agrees without coercion. To regulate dark patterns, India took the lead in 2023 by becoming the first country to address deceptive designs that manipulate consumer behaviour.

*BA LLB (HONS.), FIRST YEAR, GITARATTAN INTERNATIONAL BUSINESS, GGSIPU, DELHI.

In the year 2023, thirteen categories were identified by the Department of Consumer Affairs of India, which include the dark patterns across e-commerce platforms. The Central Consumer Protection Authority was directed to take major remedial action. The action was not merely for regulatory purposes, but as an acknowledgement of something that affects millions of users.

Many users have experienced this but are not aware whether the consent they give on these platforms is free or informed. Is this the product of deliberate manipulation?

In 2010, UX designer Harry Brignull coined the term ‘Dark Patterns’ to describe user interface designs that trick users into action and limit their choices for the benefit of platforms.¹ Since then, countdown timers, subscription traps, hidden costs revealed only at checkout, and pre-ticked consent boxes have become commonplace in digital commerce.

The article critically argues that, with India’s current existing framework, while historic, it is insufficient because, by a closed list of prohibited practices, consent in the digital market cannot be protected – it requires refined statutory provisions and redefinition of consent backed by open-ended structural prohibition and proactive enforcement.

UNDERSTANDING CONSENT IN DIGITAL MARKETS

In digital markets, consent is fundamental to every consumer transaction. According to contract law, an agreement is valid and enforceable only when both parties enter willingly with mutual consent.

According to section 14 of the Indian Contract Act, 1872, “Free consent is defined as consent that is said to be free when it is not caused by:

- Coercion, sec.15
- Undue influence, sec.16
- Fraud, sec 17.
- Misrepresentation, sec.18
- Mistake, sec. 20, 21 and 22²

¹ Harry Brignull, ‘DarkPatterns: Deception vs Honesty in UI design’ (A list apart, 29 November 2011) <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/> accessed 19 May 2026.

² *The Indian Contract Act, 1872*, s14

In digital markets, none of these categories captures what dark patterns do, yet the effect on consumer autonomy is identical. In response, section 2(47) of the Consumer Protection Act 2019 extends the principle of unfair trade practices to any method that deceives consumers in the course of a transaction.³

Why do the digital markets defy this assumption? The difference between the physical market and digital market is that, “In physical markets, consumers can ask questions; if the product is not up to the consumer's preference, a consumer can walk away or can take time to decide. While in the digital market, freedom is limited and restricted. The interface is designed by the platform; what a user sees on screen, what they order or colour, is not neutral; rather, it is engineered to produce a specific outcome that benefits the company, not the user.

The interface pattern raises concerns regarding users' privacy. The Supreme Court of India in Justice KS Puttaswamy v. Union of India⁴ addressed the question of privacy as a fundamental right.

The court held that privacy is protected under Articles 14, 19, and 21⁵ of the Indian Constitution and includes the right of individuals to regulate their own information and access to informational autonomy.

This article argues that obtaining consent through manipulative interface design violates the constitutional guarantee held in the KS Puttaswamy case that consumers have the right to informational autonomy, which is overridden before they reach the checkout page.

THE ANALYSIS OF DIGITAL DECEPTION

Dark patterns are not bad design; they are interventions operated by platforms deliberately. The guidelines by CCPA identified thirteen categories, which include false urgency, basket sneaking, confirm shaming, forced action, subscription trap, interface interference, bait and switch, drip pricing, disguised advertisement, nagging, trick questions, and rogue malware.⁶

³ Consumer Protection Act, 2019, s 2(47)

⁴ Justice *KS Puttaswamy v. Union of India* [2017]10 SCC 1(SC)

⁵ Constitution of India, Article 14,19 and 21

⁶ Central consumer protection authority, guidelines for prevention and regulation of dark patterns 2023

These thirteen categories and practices manipulate consumer consent in different ways. Three practices are particularly illustrative of how genuine choice is bypassed by interface design:⁷

Drip Pricing: A consumer selects an item at one price, proceeds with the checkout process, and at the payment stage, the user discovers that platform fees have been added. The initial price was not false; the actual disclosure of the product was engineered to ensure that the purchase is not abandoned by the consumer.

False Urgency: a lot of users must have noticed the display warning like ‘only 2 items left’, or sale ends in a few hours, which creates a fear of missing out and pressure among consumers to take immediate action. The consumer’s clicks are not entirely free, as the interface created a sense of panic and overrode the consumer's choices.

Subscription Trap: almost every platform offers a subscription. This subscription trap takes a few seconds or one or two clicks for signing up, but at the time of cancellation, the same service requires more time and navigation through multiple menus just to find the cancellation option. The design is not accidental, but rather a deliberate move to retain consumers for the platform's benefit.

Each of these practices includes a click that legally resembles consent. Looking at the categories and their patterns, the consumer did not choose them freely – they were manipulated by an interface designed to produce a specific outcome. This is precisely what section 14 of the Indian Contract Act 1872 seeks to prevent, but none of its five grounds of vitiating consent directly address manipulation through interface design.

THE REGULATORY RESPONSE: CCPA GUIDELINES 2023

In November 2023, India addressed dark patterns and came up with a direct legal response: the guidelines for the prevention and regulation of dark patterns. Section 18(2)(l) of the Consumer Protection Act 2019 encompasses guidelines that empower the CCPA to set standards to prevent unfair trade practices in e-commerce.⁸ Dark patterns of e-commerce are defined under guidelines as any practice that uses deceptive design to mislead consumers about their own

⁷ Indian Contract Act, 1872, s 14

⁸ Consumer Protection Act, 2019 (India), s 18(2) (l)

choices. For the first time, Indian law addressed manipulative interface design, backed by legal consequences.

The guidelines under CCPA enumerate thirteen categories that target specific techniques by which platforms manipulate consumers' psychology at the time of transaction.⁹ The categories represent an acknowledgement that the problem is not the fault of one bad actor; rather, it is a system-wide feature of how e-commerce platforms are built.

CCPA exercised its enforcement powers against Makemytrip India Pvt Ltd for drip pricing – the practice of concealing charges until the time of checkout, after the consumer has already invested time and attention in the booking process.¹⁰ Hence, the guidelines were not merely declaratory. The order exemplified that the CCPA is willing to hold accountable platforms, both major and small sellers. The order marked a turning point, from a framework that existed on paper to one with real consequences.

Despite this framework and enforcement, the guidelines include three limitations that prevent them from being a complete solution. First, prohibited categories are not backed by technical illustration. Second, CCPA is a single national authority overseeing millions of daily transactions in the e-commerce ecosystem; moreover, its enforcement capacity does not match that responsibility.¹¹ Third, the only remedies available are financial penalties and cease and desist orders; the platforms do not have an obligation to redesign their interface or prove their interface is compliant before a violation occurs.

THE EUROPEAN STANDARD: A COMPARATIVE PERSPECTIVE

The European Union's approach towards digital consent offers a beneficial contrast to India's framework. GDPR, or General Data Protection Regulation, requires unambiguous consent to personal data processing.¹² A pre-ticked checkbox is not sufficient for this standard because the consumer has not actively participated to indicate agreement. The Court of Justice of the European Union affirmed this in *Planet49 GmbH v Bundesverband der*

⁹ CCPA guidelines (n 3) cl 2 (I)-(xiii).

¹⁰ Central Consumer Protection Authority, 'order against makemytrip India Pvt Ltd' (Order No 11/2024, CCPA, 2024)

¹¹ Consumer Protection (E-commerce) Rules 2020 (India) r 4 (3) (b).

¹² Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJL119/1, art 7

Verbraucherzentralen¹³ holding that acceptance through a pre-selected box cannot constitute valid consent.

With the Digital Services Act 2022, the EU strengthens its framework. Article 25 prohibits platforms from operating interfaces that deceive users.¹⁴ This is not merely a list of prohibited practices in general; it is a structural prohibition that captures any manipulative design regardless of form.

In India, the thirteen listed practices cannot match this durability because the platform can design new alternatives and manipulation techniques that fall outside the listed categories. Although India's framework is historic and would benefit from adopting a similarly open-ended structural prohibition, rather than relying solely on an enumerated list.

RETHINKING CONSENT: REFORM PROPOSALS

In India, there is a need for a fundamental statutory definition of informed digital consent. The Consumer Protection Act 2019 prohibits unfair trade practices but does not define what constitutes valid consent in the digital interface context. The Act should be amended to specify the definition of consent obtained through interfaces designed to exploit cognitive biases that do not constitute valid consent for the purpose of the Act.¹⁵ Through this act, any transaction built on manufactured consent could be challenged.

India should supplement the thirteen categories list with an open-ended structural prohibition modelled on Article 25 of the EU Digital Services Act. The E-commerce rules of the year 2020 will be amended to add one general principle that no platform shall impair consumers' consent and ability to make free choices through interface design.¹⁶

Reform without regulation is incomplete. The CCPA currently operates on a complaint-driven model, which acts after a consumer files a report on a violation. The CCPA should conduct periodic audits of major e-commerce platforms, and small platforms or platforms above a threshold number of users are required to submit annual reports, which include the interface design patterns to meet the consent standards. With these reforms, the Indian framework would

¹³ Case C-673/17 Planet 49 GmbH v Bundesverband der Verbraucherzentralen [2019] ECLI:EU:C: 2019:801

¹⁴ Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJL277/1, art 25

¹⁵ Consumer Protection Act 2019, s 2(47)

¹⁶ Consumer Protection (E-commerce) Rules 2020

move from reactive enforcement of a fixed list to proactive protection of genuine consumer autonomy.

CONCLUSION

India's dark pattern guidelines 2023 marked a historic moment in consumer protection law. Manipulative interface design was first recognised as a legal wrong, and the CCPA's action against platforms like Makemytrip demonstrated that, beyond paper declarations, the framework carries real consequences. However, the consumer market cannot be future-proofed by a closed list of thirteen categories. As long as manufactured consent is treated the same as genuine consent, platforms retain an incentive to keep deceiving.

The reforms proposed in this article include a statutory definition of informed digital consent, an open-ended structural prohibition and proactive enforcement, which are not deviations from existing doctrine. As artificial intelligence and personalisation make digital manipulation more sophisticated, the law must evolve in time and treat deception as deception itself, with stricter rules backed by sanctions and legal consequences. India took its first step in 2023; the next step is ensuring that consumer consent in the digital market means something real.