



Original Research Paper

Designed to Deceive: The Hidden World of Dark Patterns

Rattan Singh^{1,2} and Simarpreet Kaur³

¹Vice-Chancellor, Jagat Guru Nanak Dev Punjab State Open University, Patiala-147001, Punjab, India

²Professor, University Institute of Legal Studies, Panjab University, Chandigarh-160014, India

³Research Scholar, University Institute of Legal Studies, Panjab University, Chandigarh-160014, India

Email: rattan67in@yahoo.com, simararnej51@gmail.com

Abstract

The rapid expansion of digital commerce and platform-based services has transformed the manner in which consumers interact with online products, services, advertisements, and data-driven technologies. Within this environment, **dark patterns** have emerged as deceptive User Interface (UI) and User Experience (UX) design practices that manipulate consumers into making choices they may not otherwise have made. By exploiting cognitive biases, information asymmetries, emotional responses, and default effects, dark patterns can influence purchasing decisions, subscriptions, consent to data processing, and other online activities, thereby undermining consumer autonomy, informed choice, privacy, and economic interests. This article examines the conceptual foundations, major forms, consumer impact, and evolving legal regulation of dark patterns, with particular emphasis on the Indian regulatory framework and comparative international approaches. It analyses prominent forms of deceptive design, including forced action, comparison prevention, confirm shaming, disguised advertisements, fake scarcity or urgency, sneaking, nagging, and preselection. The study further examines their economic, psychological, and privacy-related consequences for consumers. From a regulatory perspective, the article evaluates developments in the European Union, United States, United Kingdom, and India, including the Digital Services Act, consumer protection and data privacy frameworks, Federal Trade Commission enforcement, UK regulatory mechanisms, India's Consumer Protection Act, 2019, Consumer Protection (E-Commerce) Rules, 2020, Digital Personal Data Protection Act, 2023, and the Guidelines for Prevention and Regulation of Dark Patterns, 2023. Relevant enforcement actions and judicial and regulatory developments are also examined to illustrate the growing recognition of interface-based consumer manipulation. The article argues that existing fragmented regulatory mechanisms require stronger coordination, clearer legal definitions, effective enforcement, and greater technological oversight. It proposes explicit recognition of dark patterns as unfair digital practices, mandatory independent UI/UX audits, a specialized Digital Practices Investigation Unit, stronger penalties, transparency obligations, and enhanced consumer awareness. The study concludes that a balanced regulatory framework is necessary to preserve innovation while ensuring that digital marketplaces respect consumer autonomy, informed consent, privacy, and fair commercial practices.

Keywords:

Dark Patterns; Deceptive Design; Consumer Protection; Digital Consumer Protection; User Interface; User Experience; Consumer Autonomy; Deceptive Practices; Online Consumer Manipulation; Privacy; Informed Consent; Unfair Trade Practices; Consumer Protection Act 2019; Digital Personal Data Protection Act 2023; Dark Patterns Guidelines 2023; E-Commerce; Digital Platforms; Algorithmic Manipulation; UI/UX Ethics; Digital Regulation; Consumer Rights; Data Privacy; Regulatory Governance; Digital Fairness

*Corresponding Author:

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.129

1. INTRODUCTION

Consumers often buy unwarranted goods or reveal extensive personal information in online world. Choices that they do make but may not be as consensual as they perceive to be. Almost everyone has witnessed this and found it frustrating but not many know about the deceptive strategy and dark patterns that make them do so.

In an era marked by rapid digitalization, a prominent role is played by user interface (UI) and user experience (UX) design in influencing individual's interaction with digital platforms.¹ Frequently viewed as a neutral design, it can covertly mold consumer's viewpoints, priorities and activities. Disguised in the web of smooth and user-friendly experiences, there's hidden an escalating concern wherein digital space is increasingly transforming into a platform to deceive the consumers.² The advent of "dark patterns" design strategies, that steer or deceive consumers into inadvertent choices, presents notable setbacks to consumers' independency and transparency.³ Such design strategies by taking undue advantage of cognitive biases and information asymmetries, constantly sway individuals toward unplanned and unrequired consumer transactions, subscriptions, or dissemination of personal data.⁴

As digital platforms increasingly mediate access to information and services, addressing dark patterns has become quintessential in ensuring consumer protection. The need to secure consumers' right to free and informed choices, and protection from decisions influenced by manipulation, lies at the heart of the issue. This research article, "*Designed to Deceive: The Hidden World of Dark Patterns*," underscores the nature, impact, and regulatory framework of these deceptive design practices.

2. MEANING AND TYPES OF DARK PATTERNS

2.1 Meaning of 'Dark Patterns'

Millions of dollars are spent by e-commerce companies in developing user interfaces and navigation paths that in due course result in more profits. With the rapid progress in technology, every single day brings new techniques and way-outs for dealing with the consumers. This is to some extent justified, e-commerce companies using resources to make their product look attractive in the market, but when these sites in order to maximize their profits engage with consumers in such a way that consumers' right to free choice is affected and they manipulate their perspective in a way that makes consumers make choice detrimental to their interest; a threshold is crossed. Henry Brignull was the first one to use the term "Dark Patterns" in 2010 to demystify such practices.⁵ The Advertising Standard Council of India has defined dark pattern as, "A dark pattern is a user interface that has been crafted to trick or manipulate users into making choices that are detrimental to their interest - such as buying a more expensive product, paying more than what was initially disclosed, sharing data or making choices based on false or paid-for reviews, and so on."⁶

Dark patterns (also called deceptive patterns) are hacks applied in webpages and software applications that make consumers do things that they actually intend to, such as purchasing or signing up for any website etc. A Federal Trade Commission (FTC) staff report describes dark patterns as "design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm."⁷ Thus, dark patterns are necessarily the consumer-focused marketing strategies that take advantage of cognitive biases of the individual, driving

¹ Anu Bajaj, Krish Uppal, *et.al.*, "A Comprehensive Analysis for Dark Pattern Detection Using Structural, Visual and Textual Information" 17 *International Journal of Computer Information Systems and Industrial Management Applications* 14 (2025).

² The Advertising Standards Council of India, "Dark Patterns: The new threat to consumer protection-Discussion Document" November, 2022, available at file:///C:/Users/Dell/AppData/Local/Packages/5319275A.WhatsAppDesktop_cv1g1gvanyjgm/LocalState/sessions/A38CC90CD236C786D623605B123CC26143F3537F/transfers/2026-17/dark-patterns.pdf, (last accessed on April 25, 2026).

³ Mark Leiser, *Dark Patterns, Deceptive Design, and the Law: AI's Hidden Influence on Our Digital Experience* (Hart Publishing, Kindle edition, 2025).

⁴ Dana Abou, Alexandre Anatolievich, *et.al.*, "Unveiling the Impact of Dark Patterns on Consumer

Psychology: A Conceptual Framework Based on the Buyer Black Box Model" in A. Hamdan, *Integrating Artificial Intelligence, Security for Environmental and Business Sustainability* 197-206 (Springer, 2025).

⁵ Collin M. Gray, Cristiana Santos, *et.al.*, "An Ontology of Dark Patterns: Foundations, Definitions, and a Structure for Transdisciplinary Action" in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, Honolulu, USA, 22 pages (ACM, 2024).

⁶ *Supra* note 2.

⁷ Federal Trade Commission, "Bringing Dark Patterns to Light" in Federal Trade Commission, *Bringing Dark Patterns to Light 2* (FTC, 2022).

them to decisions, inconsistent with their intended priorities.⁸

Guidelines for Prevention and Regulation of Dark Patterns, 2023 defines dark patterns as, “Dark patterns shall mean any practices or deceptive design pattern using user interface or user experience interactions on any platform that is designed to mislead or trick users to do something they originally did not intend or want to do, by subverting or impairing the consumer autonomy, decision making or choice, amounting to misleading advertisement or unfair trade practice or violation of consumer rights.”⁹

2.2 Types of Dark Patterns

The Advertising Standards Council of India has recognized following types of dark patterns:

2.2.1 Forced Action

The strategy applied by the digital platforms makes users do something unintended in return of getting something that they want. It involves providing users what they require only in lieu of doing something in return for the provider. Many a times, an optional action is portrayed as a forced action with the use of trick wording or visual interference. In case of cookie consent interfaces, “bundled consent” strategy is often used to carry out forced action.¹⁰ “Bundled consent strategy involves integrating several agreements into a single action, rendering it hard or perhaps impossible for the user to selectively grant consent. For instance, in 2015 LinkedIn opted forced action strategy to extract email id of its users in the guise of requiring it for the website registration process. “Skip this step” button was mentioned in relatively small and too hard to notice format as compared to “Continue” option. Thus, the users were made to provide their email ids which was an optional step in reality.¹¹

2.2.2 Comparison Prevention

An ordinary prudent man generally compares the nature and price of the product before purchasing against features of other alternatives available. If this evaluation activity becomes difficult, users may give up on this comparison activity and make an unwise choice. The digital e-commerce platforms exploit this cognitive pattern and make comparison as hard as

possible.¹² This deceptive pattern is most commonly employed by mobile companies wherein they make recharge plans too complex to equate. To make it hard for the users to compare, some plans include taxes within it and other are mentioned excluding taxes. The time duration for each plan is also deliberately kept different. All this is done to make the users opt for the plan that seems to be the simplest and lucrative, though in fact, it may not be that rewarding.¹³

2.2.3 Confirm Shaming

This is another dark pattern which employs emotional manipulation to make the users do something which they otherwise would not have done. To influence users’ decision making, websites or software applications often present opt-out options in a derogatory or belittling manner, putting users in guilt or shame in not opting for the offered service or product.¹⁴ The opt out option created by eCommerce website mimedic.com clearly qualifies the test of confirm shaming dark pattern. In 2018, in order to seek permissions from the users for sending notifications to the users for its website, Mymedic labelled the opt out button as, “No, I don’t want to stay alive” or “No, I prefer to bleed to death”. Such types of notifications can lead people to traumas if they happen to opt out.¹⁵

2.2.4 Disguised Ads

This type of dark pattern waters down the line between actual content and advertisement, creating ambiguity for the users. The user is made to believe that they are clicking on an interface element or native content but in reality, it is a disguised advertisement. Thus, website owners in order to serve their ulterior motive of generating more revenue from ads befool the general public.¹⁶ A famous software download website, Softpedia, employs these disguised ads strategy by portraying disguised ads on their software download pages. The above-mentioned software displays advertisements with a notable download button that looks like the actual download button for the required software. This similarity makes users to mistakenly click on the ad, considering they are downloading the software.¹⁷

2.2.5 Fake Scarcity or Fake Urgency

⁸ *Supra* note 2 at 14.

⁹ The Guidelines for Prevention and Regulation of Dark Patterns, 2023.

¹⁰ Deceptive Patterns, “Forced Action” available at <https://www.deceptive.design/types/forced-action> (last visited on April 25, 2026).

¹¹ Deceptive Patterns, “Forced Action” available at <https://www.deceptive.design/types/forced-action> (last visited on April 25, 2026).

¹² Deceptive Patterns, “Comparison Prevention” available at

<https://www.deceptive.design/types/comparison-prevention> (last visited on April 25, 2026).

¹³ *Ibid.*

¹⁴ Deceptive Patterns, “Confirmshaming” available at <https://www.deceptive.design/types/confirmshaming> (last visited on April 25, 2026).

¹⁵ *Ibid.*

¹⁶ Deceptive Patterns, “Disguised Ads” available at <https://www.deceptive.design/types/disguised-ads> (last visited on April 25, 2026).

¹⁷ *Ibid.*

Herein, fake scarcity or popularity is created to pressurize the user to accomplish an action without due consideration.¹⁸ This is the most common type of dark pattern used by e-commerce websites like amazon, flipkart etc. “2 slots left” or “limited time sale” are some examples of the labels used to create pressure on the consumer to purchase the commodity as soon as possible, failing which, they won’t be able to buy the same.

2.2.6 Sneaking

Intentional withholding or concealment of relevant information from the user such as additional costs or unintended consequences with the aim to manipulate and influence the users into taking an action which they would not have otherwise taken. This consumer deception technique is known as sneaking. The user is made to enter into a transaction on the basis of false pretences. The unwanted subscription or a commodity sneaked into users’ shopping cart is a perfect example of sneaking. If user notices it, then he needs to make an extra effort to remove from the bag and if he doesn’t notice, then he falls into the trap of digital platforms.

2.2.7 Nagging

When users want to do something, but they are continuously interrupted by the requests to do something else which may be disadvantageous to them, it is called nagging.¹⁹ In 2018, Instagram sent repeated requests to the users to turn on the notifications and this continued over a period of months. The users were not provided with the direct ‘reject’ button but ‘Not Now’ was available to them and this allowed Instagram to send same requests again and again. The practice is regarded as aggressive nagging by Instagram.²⁰

2.2.8 Preselection

Preselection makes use of the default effect cognitive bias, wherein people gravitate toward the options already selected for them. Owners of websites and software applications exploit this by using tactics like pre-ticked checkboxes, automatically added items

in carts, or pre-selected steps in a process. This delivers results as users may not discern or fully comprehend the consequences²¹. It can also be reinforced by other biases, such as social proof bias (suggesting others would accept the default) or authority bias (using authority figures to influence decisions). This pattern was used during the 2020 Donald Trump 2020 presidential campaign; wherein preselected checkboxes led many donors to make involuntary recurring and additional payments.²²

3. IMPACT ON CONSUMERS

The dark patterns affect the consumers both economically and psychologically. Economically, the purchase of unintended or unwarranted products and services financially drain the consumers. Psychologically, these patterns undermine right to free of choice of the consumers. Research by the Consumer Policy Research Centre (Australia) and OECD shows that dark patterns mislead users by exploiting impulsivity, confusion, and social pressure.²³

In addition to this, dark patterns also pose threat to the privacy of the individuals. The users are often nagged into disclosing of personal details with no full and clear understanding of the consequences. In this digital era, the digital footprints remain forever and internet never forgets anything. All this undermines the principle of informed consent and exposes the user to privacy attacks.

4. LEGAL AND REGULATORY FRAMEWORK

4.1 International Perspective

4.1.1 European Union²⁴

There is no uniform definition of dark patterns under European Union law. *The Digital Services Act* (DSA) explains them as, “Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions.”²⁵ The *EU Consumer law fitness check* identifies them as unfair interface designs affecting

¹⁸ Deceptive Patterns, “Fake Scarcity” available at <https://www.deceptive.design/types/fake-scarcity> (last visited on 25th April 2026).

¹⁹ Deceptive Patterns, “Nagging” available at <https://www.deceptive.design/types/nagging> (last visited on 25th April 2026).

²⁰ *Ibid.*

²¹ Deceptive Patterns, “Preselection” available at <https://www.deceptive.design/types/preselection> (last visited on 25th April 2026).

²² *Ibid.*

²³ OECD, “Dark Commercial Patterns” available at <https://www.oecd.org/content/dam/oecd/en/publicatio>

[ns/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf) (last visited on 25th April 2026).

²⁴ European Parliamentary Research Service (EPRS), “At a Glance: Regulating Dark Patterns in the EU: Towards Digital Fairness” in European Parliament, *At a Glance* 767191 (European Parliament, 2025).

²⁵ 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). Official Journal of the European Union L 277, 27.10.2022.

decisions.²⁶ Both definitions emphasize manipulation and harmful outcomes.

Dark patterns have been primarily dealt under the *Unfair Commercial Practices Directive*²⁷ (UCPD), which forbids misleading and aggressive practices however, does not clearly specify digital interfaces. In addition to this, other laws like the General Data Protection Regulation²⁸ (GDPR) encompass related issues, which at times overlap and create legal ambiguity. For instance, if a technique violates GDPR, it is dealt with under GDPR and not DSA.

Apart from these, there are some other significant EU laws that cover within its scope dark patterns. *The Artificial Intelligence Act*²⁹ prohibits manipulative or deceptive AI practices. *The Digital Markets Act*³⁰ incorporates anti-circumvention rules. *The Data Act*³¹ and amendments to the Consumer Rights Directive also set limitations on the manipulative interface design. But, this piecemeal framework risks inconsistent enforcement. There is a need for clearer definitions and stronger enforcement mechanism in EU for effectively curbing such deceptive patterns.

4.1.2 United States of America

The Federal Trade Commission (FTC) is primarily responsible in USA for the regulation of dark patterns. Coupled with this, there are state level data privacy statutes that are used for governing dark patterns. The

FTC has issued warning to the businesses against user interface designs that mislead and manipulate users into making decisions that they would not have otherwise made.³²

Not only this, but FTC has also actively enforced prevalent consumer protection law, specifically provisions pertaining to the prohibition on unfair or deceptive acts or practices under Federal Trade Commission Act, by holding violators accountable.³³ These enforcement measures have resulted in notable financial penalties, including settlement payments and consumer restitution, depicting strong regulatory scrutiny of such practices.

Data privacy legislations at the state level have further emboldened the regulatory framework. *The California Consumer Privacy Act*³⁴ (CCPA) mandates businesses to take clear and informed consent for data processing, secure transparency in user choices, and shun manipulative interface designs. Likewise, the *California Privacy Rights Act*³⁵ (CPRA) and the *Colorado Privacy Act*³⁶ clearly provide that consent obtained through dark patterns is no consent and hence invalid.

Thus, USA is devoid of a coherent legislative framework dealing with dark patterns but Federal Trade Commission and state level legislations, cumulatively protect users against dark patterns designed to deceive the users.

4.1.3 United Kingdom (UK)

²⁶ European Digital Policy Initiative, “Digital Fairness Act – Fitness Check”, available at: <https://edpi.eu/digital-fairness-act-fitness-check> (last visited on April 26, 2026).

²⁷ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive), available at: <https://eur-lex.europa.eu/eli/dir/2005/29/oj/eng> (last visited on April 26, 2026).

²⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), available at: <https://gdpr.eu.org/full/full.pdf> (last visited on April 26, 2026).

²⁹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (last visited on April 26, 2026).

³⁰ European Commission, “Digital Markets Act”, available at: https://digital-markets-act.ec.europa.eu/index_en (last visited on April 26, 2026).

³¹ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), available at: <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng> (last visited on April 26, 2026).

³² Nessa Khandaker, Lynn Parker Dupree and Jennifer E. Fried, “Dark Patterns Regulation in the UK and US”, Finnegan (7 May 2025), available at: <https://www.finnegan.com/en/insights/articles/dark-patterns-regulation-in-the-uk-and-us.html> (last visited on April 26, 2026).

³³ Federal Trade Commission (FTC), “Federal Trade Commission – Protecting America’s Consumers”, available at: <https://www.ftc.gov/> (last visited on April 26, 2026).

³⁴ California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (as amended) (United States of America).

³⁵ California Privacy Rights Act of 2020, amending Cal. Civ. Code §§ 1798.100 et seq. (United States of America).

³⁶ Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 to 6-1-1313 (United States of America).

The Advertising Standards Authority (ASA) is an independent authority in UK that oversees advertising in UK and can take measures against companies employing dark patterns to delude the consumers.³⁷ It has prohibited ads that violate rules and regulations on deceptive advertising and set out guidance accentuating transparency in fields like subscriptions, pricing, and promotions.

There are two other authorities, the Information Commissioner's Office³⁸ (ICO) and the Competition and Markets Authority³⁹, that study effect of dark patterns on user data. These authorities caution the businesses against deceptive patterns like complex cookie refusals, default settings that prefer data sharing and consolidated privacy choices. Such strategies breach UK GDPR principles of fairness and transparency. The ICO can penalize the offenders with fines of up to £17.5 million or 4% of global turnover, along with reputational penalties like public warnings.⁴⁰

4.2 Indian Perspective

At the earliest stages, India has only *Information Technology Act, 2000*⁴¹ to deal with dark patterns but it lacked provisions specifically relating to manipulative UI designs and deceptive consent. Thus, there was a legal vacuum in the regulatory framework pertaining to dark patterns in India's digital environment. Notable progress occurred with the enforcement of the *Consumer Protection Act, 2019*⁴², which expanded the scope of unfair trade practices and constituted the Central Consumer Protection Authority (CCPA), though it did not specifically define dark patterns.⁴³

The framework was further clarified through the *E-Commerce Rules, 2020*⁴⁴, that mandated explicit

user's consent and prohibited strategies like pre-ticked checkboxes. *The Digital Personal Data Protection Act, 2023*⁴⁵ reinforced user autonomy by mandating clear consent and permitting withdrawal.

A key milestone was reached with the *Guidelines for Prevention and Regulation of Dark Patterns, 2023*⁴⁶, which comprehensively apply to digital platforms, advertisers, and sellers⁴⁷. These guidelines have been issued by the Central Consumer Protection Authority under the powers conferred by section 18 of the Consumer Protection Act, 2023. These Guidelines prohibit all dark patterns⁴⁸ but fail to remove ambiguity in cross-border enforcement and risk overregulation if given too wide interpretation.

Enforcement has strengthened since November 2023. In May 2025, under Pralhad Joshi, stakeholders across industries pledged compliance and awareness efforts, supported by a Joint Working Group. Tech-driven tools like the Jagriti Dashboard and Jago Grahak Jago safety rating system enhance monitoring and consumer reporting.⁴⁹

Over 50 platforms have been directed by the CCPA on June 7, 2025 to conduct self-audits and file compliance declarations. Multiple notices have also been issued for violations, warning of strict penalties for non-compliance by CCPA.⁵⁰

The Advertising Standards Council of India (ASCI), a self-regulatory organization established in 1985, has pre-emptively identified and called attention to the digital advertisements that employ disguised content like native editorial, misleading discounts and pre-checked data sharing options.⁵¹ Though without legal force, ASCI's guidelines have been used to caution the advertisers and to persuade the platforms into self-regulation.

³⁷ Advertising Standards Authority (ASA), "Home", available at: <https://www.asa.org.uk/> (last visited on April 26, 2026).

³⁸ Information Commissioner's Office (ICO), "Home", available at: <https://ico.org.uk/> (last visited on April 26, 2026).

³⁹ Competition and Markets Authority (CMA), "Home", available at: <https://www.gov.uk/government/organisations/competition-and-markets-authority> (last visited on April 26, 2026).

⁴⁰ *Supra* note 32.

⁴¹ Information Technology Act, 2000, Act No. 21 of 2000.

⁴² Consumer Protection Act, 2019, Act No. 35 of 2019.

⁴³ Stella Joseph, Prakhil Mishra and Sonalika Khatri, "India's Evolving Framework for the Regulation of

Dark Patterns", Bar & Bench, available at: <https://www.barandbench.com/view-point/indias-evolving-framework-for-the-regulation-of-dark-patterns> (last visited on April 26, 2026).

⁴⁴ Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 462(E), Ministry of Consumer Affairs, Food and Public Distribution.

⁴⁵ Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.

⁴⁶ Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, Notification No. CCPA-2023.

⁴⁷ *Id.*, s.3.

⁴⁸ *Supra* note 46, s.4.

⁴⁹ *Supra* note 43.

⁵⁰ *Supra* note 43.

⁵¹ Advertising Standards Council of India (ASCI), "Home", available at: <https://www.ascionline.in/> (last visited on April 26, 2026).

5. JUDICIAL APPROACH AND CASE LAWS

5.1 International judicial framework

Judiciary too has stepped in to curb the menace of dark patterns, and through its interpretations the businesses engaging in such tactics are penalized.

5.1.1 *Epic Games v. FTC (2022), United States*⁵²

In this notable judgment, Interface Manipulation has been recognized as a deceptive pattern to mislead the consumers under US law. Epic Games was penalized by the Federal Trade Commission with a fine of \$245 million for engaging in deceptive interfaces that fooled the players and made them make unintended in-game purchases.

5.1.3 *Booking.com and European Commission Enforcement*⁵³

Booking.com had been forced in 2020 by the European Commission to put an end to its false urgency tactics along with countdown timers and in 2020, the European Commission forced Booking.com to cease its use of false urgency tactics, including countdown timers and misleading stock warnings. The European Union's consumer protection framework regards such practices as aggressive commercial practices violating the Unfair Commercial Practices Directive.

5.2 Indian Case laws

In India, though there is no landmark ruling specifically dealing with "dark patterns" but the courts and consumer commissions have on various occasions protected the consumers against unfair trade practices opted by the big tech giants. Some of the prominent instances wherein businesses have employed practices resembling dark patterns are:

5.2.1 *MakeMyTrip India Pvt. Ltd. & Ors. v. GoIbibo & Ors.*⁵⁴

It was contended that MakeMyTrip and GoIbibo had been indulged in anti-competitive practices and price manipulation tactics, false discounting and deceptive representations to befool the customers. Following this, the Competition Commission of India ordered the probe against the above-mentioned companies. The allegations alleged

typically falls under the category of bait-and-switch and drip pricing patterns. Though, the commission has viewed the entire case from the prism of competition lens, it paved the way for scrutinization of interface-level design abuse.

5.2.2 *Zomato Gold and Swiggy Super Complaints*⁵⁵

As of now, consumer forums have been flooded with complaints against Zomato's Gold membership and Swiggy Super, wherein users are first lured by the offers but thereafter face restrictions and misleading renewal clauses making it difficult to opt out. These tactics employed fall under the category of forced continuity and roach motel patterns, wherein signing up is easy but cancellation is deliberately made difficult.

5.2.3 *Union of India v. Ola & Uber (Delhi HC, 2016)*

In this case, Delhi High Court has opportunity to examine allegations against ride hailing services for making use of deceptive dynamic pricing. While not formally recognized as dark patterns, the non-transparent surge model nearly matches disguised pricing and sneaking, more so when full fare is made known only post-booking.⁵⁶

6. RECOMMENDATIONS AND POLICY SUGGESTIONS

6.1 Clear recognition and definition

To effectively regulate dark patterns, there's an urgent need to recognize dark patterns explicitly within the law books. India needs to formally define dark patterns under the Consumer Protection Act, 2019, classifying them as unfair trade practices, misrepresentation, and consent manipulation. This would ensure effective enforcement by key regulators such as Central Consumer Protection Authority, Competition Commission of India and MeitY.

6.2 Mandatory UI/UX audits

There is the need to introduce mandatory User Interface/User Experience audits by independent bodies to inspect subscription flows, default configuration, order-completion processes and consent mechanisms. The platforms should also be

⁵² Federal Trade Commission, *FTC v. Epic Games: Epic to Pay \$520 Million Over Allegations of Privacy Violations and Dark Patterns*, Press Release (Dec. 19, 2022), available at: <https://www.ftc.gov/news-events/news/press-releases/2022/12/epic-games-pay-520-million-settle-ftc-allegations>.

⁵³ European Commission, *Booking.com Consumer Complaint Resolution (2020)*, available at <https://ec.europa.eu/info/live-work-travel-eu/consumers>.

⁵⁴ Competition Comm'n of India, Case No. 14 of 2019 – *MakeMyTrip India Pvt. Ltd. & Ors. v. GoIbibo & Ors.*,

<https://www.cci.gov.in/sites/default/files/14-of-2019.pdf> (last visited July 14, 2025).

⁵⁵ Lawful Legal, *Dark Patterns in E-Commerce: Defeating Legal Expectations*, LAWFUL LEGAL (2023), <https://lawfullegal.in/dark-patterns-defeating-in-e-commerce-legal-expectations-and-consumer-protection/>. (last visited on April 26, 2026).

⁵⁶ *Union of India v. Ola & Uber*, W.P.(C) 6485/2016 (Del. HC).

made to publish transparency reports on prominent design changes that may affect users' choice.⁵⁷

6.3 Setting up of Digital Practices Investigation Unit and stringent penalties

A committed Digital Practices Investigation Unit with design and behavioral expertise needs to be set up. Also, there's the requirement to make the penalties more stringent as well as enforcement mechanism stronger.⁵⁸

6.4 Consumer Awareness

The efforts would be in vain unless and until consumers themselves are aware. Through public campaigns and school curricula digital literacy needs to be promoted.

7. CONCLUSION

Today, we all depend on the digital world for satisfaction of our needs, be it recreational, educational or for shopping. In return of being there in the online world, we all have succumbed our privacy and control over things in one way or the other. The digital marketplace, in theory, does have choice to exit, view other alternative options using filters, as well as devising one's own priorities but in reality, the algorithms and user-manipulation techniques push the users in a certain direction only. Dark patterns are those deceptive techniques that trick the users in doing something which otherwise they would not have done. The online space today is replete with these dark patterns, designed to deceive and befool the consumers and maximize the profits. The lack of regulatory framework specifically dealing with these deceptive patterns, make consumers view online space with suspicion. Though, it is not possible to put the internet and e-commerce genie back into bottle but it could be made less predatory through proper law enforcement.

⁵⁷ Manasi Yamgar, "Dark Patterns in Online Shopping and Consumer Deception", Legal Vidhiya, available at: <https://legalvidhiya.com/tag/dark-patterns-in->

[online-shopping-and-consumer-deception/](#) (last visited on April 26, 2026).

⁵⁸ *Ibid.*