
DARK PATTERNS: A LURKING MENACE TO CONSUMER'S SHIELD

Navtej Tyagi & Navjot Tyagi, Babu Banarasi Das University, Lucknow.

ABSTRACT

This comprehensive article delves into the intriguing realm of consumer protection, shedding light on the emerging threat posed by dark patterns - deceptive design techniques used to manipulate user behavior. By exploring the definition and various types of dark patterns, this study uncovers the pervasive ways in which companies employ these manipulative tactics to influence consumer decision-making. With a specific focus on both domestic and international perspectives, the essay delves into the regulatory landscape surrounding dark patterns. This article provides valuable insights into the prevalence and impact of dark patterns on consumer trust and well-being. Furthermore, it offers practical recommendations for policymakers, businesses, and consumers to mitigate the prevalence of these deceptive practices and foster a more transparent and ethical digital environment. By raising awareness about dark patterns, we can ensure that the rights of the vigilant are upheld, for '*vigilantibus non dormientibus jura subveniunt*' - the law aids those who are watchful. Join us on this enlightening journey as we unravel the covert strategies employed by businesses and empower consumers to make informed choices in the face of dark patterns.

Keywords: Consumer protection, Dark Patterns, Legal framework, Regulatory landscape, Domestic & International Perspective.

INTRODUCTION

“Electronics is clearly the winner of the day.”- John Ford

In this era of the twenty first century we find ourselves immersed in the e-century, where technological advancements and the marvels of digitalization reign supreme. The vast realm of the online digital world has captured our collective admiration and dependence. It stands as a virtual universe, a sanctuary to which we constantly turn for our myriad needs, be it education, shopping, banking, communication, or entertainment. Indeed, it has become an integral facet of the modern consumer's life, exerting a profound influence on their consumption of information, products, and services. With the surge in electronic commerce, safeguarding the well-being of consumers has assumed an unprecedented level of significance.

Earl Warren said – ***“The Fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual.”***

In the realm of contemporary e-commerce, it is a common practice for a multitude of companies to allocate substantial financial resources towards the meticulous crafting of user interfaces (UI), with the ultimate goal of augmenting their business endeavors. Alas! these very interfaces possess the potential to guide consumers towards choices that may not necessarily align with their best interests. **Dr. Harry Brignull**¹, a User Experience (UX) Director came up with the term **“Dark Patterns”** in **2010** to describe these sneaky practices. Each passing day brings forth novel technological innovations that offer fresh avenues for engaging with consumers. However, when these methods are employed in a manner that steers individuals towards choices that undermine their own welfare, an undeniable predicament arises. In the month of October in the year 2022, the esteemed Organization for Economic Cooperation and Development (OECD) published a paper, which revealed that a staggering 57.4% of the cookie consent notices on Europe's websites employ designs that surreptitiously coax users into compromising their privacy². Even tech behemoths such as LinkedIn, Amazon, Apple, and Google have, at certain junctures, been associated with the utilization of deceptive patterns. Hence, it becomes an imperative to foster a transparent and ethical digital environment that places paramount importance on user rights and well-being. This article endeavors to dissect

¹ Founder of the Deceptive Patterns Initiative & Head of Innovation at Smart Pension.

² OECD, *Dark commercial patterns*, 336 OECD Digital Economy Papers, 5, 19 (2022).

the intricacies of dark patterns, examining both the national and global landscape, the challenges faced by consumers, and charting a path towards a brighter future.

LET'S DIVE INTO THE MEANING OF DARK PATTERNS

Dark Patterns or Deceptive Patterns are unethical strategies or manipulative UI/ UX design techniques employed by websites, apps, and other digital platforms. Their sole purpose is to deliberately mislead unsuspecting consumers and induce them to perform actions that run contrary to their original intentions, often to their detriment. Such patterns are cunningly devised to suppress activities that are deemed unfavorable to the interests of e-commerce companies³.

They exploit the very fabric of our cognitive and behavioral biases, leveraging psychological principles to sway our decisions.

Picture this, if you will: In the midst of your blissful perusal of an online hotel booking platform, you are suddenly accosted by false urgency, proclaiming the scarcity of available rooms with the audacious claim of "Only 3 rooms left! Book now for a luxurious stay!" or when you're booking a flight ticket and boom, they automatically add travel insurance. These are a mere glimpse into the treacherous tactics employed by the titans of the technology industry, all in the pursuit of amassing greater wealth.

KINDS OF DARK PATTERNS SPECIFIED BY MINISTRY OF CONSUMER AFFAIRS, FOOD AND PUBLIC DISTRIBUTION⁴, GOVERNMENT OF INDIA

1) False Urgency : Creates a sense of urgency to persuade consumers to make an immediate purchase.

Example – A purveyor of goods and services resorts to the nefarious stratagem of fabricating temporal exigency to manipulate potential patrons. This Machiavellian merchant, in an ostentatious display of linguistic prowess, proclaims a sale of unparalleled exclusivity, ostensibly confined to a circumscribed period, solely accessible to a select

³ This Definition is attempted by synthesizing various definitions on dark patterns.

⁴ Government of India, Ministry of Consumer Affairs, Food and Public Distribution, The Guidelines for Prevention and Regulation of Dark Patterns, 2023, 783 (November 30, 2023)

coterie of discerning individuals.

- 2) *Basket Sneaking / Sneak into Basket*: This dark pattern sneakily adds extra products or services to the shopping cart without user's consent which makes the user pay more than he desired.

Example – Imagine a scenario where an esteemed individual decides to partake in the indulgence of a solitary salon service. However, to their dismay, as they proceed to complete the transaction, an audacious subscription to the salon service is surreptitiously appended without their express consent or volition.

- 3) *Confirm Shaming*: It utilizes several methods to create shame or guilt in the minds of users which leads them to opt something benefitting the companies or makes the consumers abstain from cancelling a product or service already subscribed.

Example- My Medic an online platform used a deceptive pattern to get the permission for sending notifications in the manner “Allow or No, I don't want to stay alive”

- 4) *Forced Action*: Compels consumers to perform an action to get something they want.

Example – In 2015, LinkedIn made it seem mandatory to provide email addresses during registration, but their real goal was to access users' inboxes and collect more addresses. They hid the option to decline as a small "skip this step" link.

- 5) *Subscription Trap*: Websites make it super easy to sign up for a service, but when it comes to cancelling, they hide the option or make it a complicated process with multiple steps.
- 6) *Interface Interference*: Using tactics that make it really challenging for consumers to do certain things, like cancelling a subscription or deleting an account. This makes the process intentionally difficult and confusing.

Example- When you tap the "X" to close a pop-up, but it opens another ad instead. It's like they're trying to trick you into more ads.

- 7) *Bait and Switch*: E-commerce companies promise one thing in their advertisements, but what the consumers get actually is an unexpected product/service. Sometimes, it's even of

a lower quality than what they advertised.

- 8) *Drip Pricing*: Companies advertise a product with a certain price, but as you go through the buying process, they reveal additional charges that you weren't aware of initially.
- 9) *Disguised advertisement*: They are sneaky advertisements that try to blend in other types of content. They can look like news articles or even stuff created by users themselves. It also includes misleading advertisements as mentioned in **Section 2(28) of the Consumer Protection Act 2019**⁵. The “**Guidelines for Prevention of Misleading Advertisements, 2022**”⁶ apply to them too.
- 10) *Nagging*: A dark pattern due to which users often find themselves bombarded with a flurry of requests, information, options, etc. These distractions can be unrelated to the original purchase and interrupt the intended transaction.

HOW EXACTLY DO COMPANIES EMPLOY DARK PATTERNS?

Some social media companies use dark patterns to slyly shape the consumer's choices. Here are a few instances:

- 1) Some Dating apps have made it trickier to delete accounts. Instead of a straightforward 'Yes' or 'No' options, they make users to manually type the word “delete” to confirm the deletion. It can definitely be more challenging and time-consuming for users who want to remove their accounts.
- 2) On the esteemed platform of LinkedIn, it is not uncommon for its distinguished users to encounter unsolicited, sponsored missives from influential personas. However, the process of disabling this feature proves to be an arduous endeavor, replete with intricate steps that necessitate a comprehensive understanding of the platform's controls.
- 3) YouTube can be a bit annoying with those pop-ups for YouTube Premium. They cover the final seconds of a video with thumbnails, which can be frustrating when you're trying to

⁵ The Consumer Protection Act, 2019, §2(28), Act No. 35, Act of Parliament, 2019(India).

⁶ Government of India, Ministry of Consumer Affairs, Food and Public Distribution, The Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022, 291 (June 9, 2022)

watch till the end.

- 4) In the European Union, Amazon received backlash for the complex cancellation process for Amazon Prime Subscription. However, in 2022, Amazon made the cancellation process simpler for online customers in European countries.
- 5) In the past, Trip advisor was criticized for displaying misleading information about hotel availability. They used a dark pattern called "misdirection" by showing a hotel as fully booked, even when it wasn't, to create a sense of urgency and encourage users to make quicker bookings.
- 6) Ticketmaster has been accused of using dark patterns to create a sense of urgency during the ticket purchasing process. This includes showing limited availability or countdown timers, pressuring users to make quick decisions.
- 7) Online Subscription Services like streaming platforms or magazine subscriptions have been known to use dark patterns to make it difficult for users to cancel their subscriptions. They may hide the cancellation option or require multiple steps, hoping to retain customers for longer.

WHY SHOULD INTERNET USERS GET WORRIED ABOUT DARK PATTERNS?

Dark Patterns are indeed a cause for concern, as they detrimentally impact users' online experiences, exploit their vulnerabilities, and manipulate their actions and choices, thereby resulting in unintended financial ramifications and the improper utilization of personal data. These insidious tactics not only engender a protracted and convoluted completion of seemingly simple tasks but also ensnare users into inadvertent purchases or the divulgence of excessive personal information. Particularly intrusive patterns, such as confirm shaming, exert undue pressure upon consumers to acquiesce to privacy-compromising settings. Consequently, they undermine the bedrock of trust and confidence within the marketplace. According to the comprehensive findings of the United States Federal Trade Commission's Report, the proliferation of augmented reality (AR) and virtual reality (VR) platforms and devices may provide a fertile ground for the insinuation of dark patterns into these emerging realms of communication.

WHAT ARE THE ACTIONS THAT INDIA HAS TAKEN TO ADDRESS THIS ISSUE?

Constitutional Provisions

While there isn't a specific constitutional Article in India that directly addresses dark patterns, there are provisions that can protect individuals' rights in the digital space. Take, for instance, **Article 21**⁷, which guarantees the *Right to Life and Personal Liberty*, which encompasses Right to privacy⁸ and protection against deceptive practices. Additionally, **Article 19(1)(a)**⁹ ensures the *Freedom of Speech and Expression*, which is highly relevant when it comes to ensuring transparency¹⁰ and fairness online. It is important to note that any violation of the Right to Privacy must meet the triple test¹¹: a legitimate aim, proportionality, and legality. Dark patterns do not fulfill these criteria, except for benefitting commercial platforms.

Recognizing this, the Indian government has taken up steps to introduce different regulations and laws to curb the use of dark patterns so that they do not infringe upon citizen's Right to Privacy.

The Consumer Protection Act, 2019 (CPA, 2019)

The Consumer Rights¹² encompass the following facets: protection against hazardous goods or services, information about quality, price, and protection against unfair practices, access to a variety of competitive goods or services, assurance that consumer interests will be considered, redress against unfair trade practices, consumer awareness. However, by the implementation of the surreptitious 'sneak into basket' technique, e-commerce platforms flagrantly infringe upon the consumer's fundamental entitlement **to be duly informed**. This insidious pattern entails the inclusion of supplementary items into the basket unbeknownst to the unsuspecting consumer. Another instance of a pernicious design strategy impeding the consumer's **freedom of choice** is the utilization of pre-selected option boxes. The recognition that these pre-selected boxes can exploit the user's cognitive bias prompted the Insurance and Regulatory

⁷ INDIA CONST. art. 21.

⁸ K.S. Puttaswamy (Retd.) v. Union of India, AIR 2017 SC 4161; Ram Jethmalani v. Union of India, (2011) 8 SCC 1: JT 2011 (7) SC 104: (2011) 6 SCALE 691.

⁹ INDIA CONST. art. 19, cl.1(a).

¹⁰ This means that individuals have the right to express their opinions, share information, and seek transparency from the government or other entities.

¹¹ K.S. Puttaswamy v. Union of India(2017) 10 SCC 1.

¹² The Consumer Protection Act, 2019, §.2(9), Act No. 35, Act of Parliament 2019(India).

Development Authority of India (IRDAI)¹³ to prohibit the utilization of such practices by travel insurance portals¹⁴.

According to a press release¹⁵ by the **Department of Consumer Affairs**¹⁶, when shopping online, reviews are super important since we can't physically see products. But fake and misleading reviews violate our Right to be Informed under **the Consumer Protection Act, 2019**.

Therefore to ensure consumers' safety, The Department of Consumer Affairs in India has warned online marketplaces about using unfair trade practices (UTPs)¹⁷. They're specifically concerned about dark patterns in user interfaces that manipulate consumer choice and hinder their right to be well informed. It's all about protecting consumers under the Consumer Protection Act 2019.

The Department is also now categorizing the complaints they receive on the **National Consumer Helpline (1915 or 1800-11-4000)** to gather information about dark patterns. This information can then be used by **the Central Consumer Protection Authority**¹⁸ to take action under the Consumer Protection Act, 2019.

The Department introduced the 2020 Consumer Protection (E-Commerce) Rules¹⁹. These rules define responsibilities, specify liabilities, and address customer grievances in e-commerce. **Rule 5(4)** of these Rules mandates that e-commerce entities abstain from disseminating or facilitating the promotion of deceptive advertisements.

¹³ The Insurance Regulatory and Development Authority of India (IRDAI), a revered statutory entity, stands as a formidable guardian, dedicated to the preservation of policyholders' interests, as well as the regulation, promotion, and facilitation of the harmonious expansion of the insurance sector within the nation of India.

¹⁴IRDAI, Ref No.-IRDAI/HL T/CIR/MISC/174/09/2019, (Sept. 27, 2019).

¹⁵Ministry of Consumer Affairs, Food and Public Distribution, *Fake Reviews on E-commerce Platforms under centre's radar*, May 26, 2022, <https://pib.gov.in/PressReleasePage.aspx?PRID=1828485> (last visited on Jan 23, 2024).

¹⁶ Department of Consumer Affairs is one of the two Departments under the Ministry of Consumer Affairs, Food & Public Distribution, Government of India. It was constituted as a separate Department in June 1997 to give a fillip to the nascent consumer movement in India. See, Ministry of Consumer Affairs, Food and Public Distribution *About DCA*, <https://consumeraffairs.nic.in/about-us/about-dca> (last visited on Jan 23, 2024).

¹⁷ The Consumer Protection Act, 2019, §.2(47), Act No. 35, Act of Parliament 2019(India).

¹⁸The Consumer Protection Act, 2019, §10, Act No. 35, Act of Parliament 2019(India). As provided in Section 10 of the Consumer Protection Act, 2019 the Central Consumer Protection Authority was established on 24th July, 2020.

¹⁹ Government of India, Ministry of Consumer Affairs, Food and Public Distribution, *The Consumer Protection (E-Commerce) Rules, 2020*, 358 (July 23, 2020)

The Guidelines issued under this Act like **the Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements 2022**²⁰ might also address the issue of dark patterns.

Upon meticulous scrutiny of **Section 2(11)(ii)**²¹ in conjunction with **Section 2(28)(iv)**²² of the Act, one can discern that the legislative framework designates a service as "deficient" and imposes penalties for the deliberate withholding of pertinent information. The latter provision characterizes such conduct as "misleading advertisement". **Section 89**²³ prescribes the punishment for false or misleading advertisement which comes under the category of disguised advertisements (a type of dark patterns). In India, one way to spot a dark pattern in UI/UX is if it's intentionally designed to mislead. But determining intention can be challenging in every case. It depends on how **the Central Consumer Protection Authority** interprets it.

On 30th November, 2023 the **Central Consumer Protection Authority**, in the exercise of the powers²⁴ conferred by the Consumer Protection Act 2019, issued "**Guidelines for Prevention and Regulation of Dark Patterns, 2023**"²⁵. These Guidelines are applicable to all platforms that offer goods and services in India on a regular basis.

The Advertising Standards Council of India (ASCI)²⁶ has provided guidelines against the dark patterns. It uses its current code on misleading advertisements to address these concerns. This code covers all media, including online advertising on websites and social media platforms.

The Digital Personal Data Protection Act, 2023

This Act recognizes and addresses the deceptive patterns that coerce users into sharing personal info. It emphasizes explicit consent and ensuring user control over their data. It's all

²⁰ Government of India, Ministry of Consumer Affairs, Food and Public Distribution, The Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022, 291 (June 9, 2022). The Central Consumer Protection Authority had notified these guidelines on 9th June 2022. These guidelines include things like: a) making sure advertisements are truthful and accurate, b) setting rules for bait advertisements and free claim advertisements, and c) outlining the responsibilities of manufactures, service providers, advertisers, and advertising agencies.

²¹ The Consumer Protection Act, 2019, §2 cl.11(ii), Act No. 35, Act of Parliament 2019(India).

²² The Consumer Protection Act, 2019, §.2 cl.28(iv), Act No. 35, Act of Parliament 2019(India).

²³ The Consumer Protection Act, 2019, §.89, Act No. 35, Act of Parliament 2019(India).

²⁴ The Consumer Protection Act, 2019, §.18, Act No. 35, Act of Parliament 2019(India).

²⁵ Government of India, Ministry of Consumer Affairs, Food and Public Distribution, The Guidelines for Prevention and Regulation of Dark Patterns, 2023, 783 (November 30, 2023)

²⁶ The ASCI was established in 1985. It a self regulatory body of the Indian Advertising industry

about making sure that consent is crystal clear and not just assumptions or opt-out methods.

The Information Technology (Reasonable Security Practices & Procedures & Sensitive Personal Data or Information) Rules 2011 (“SPDI” Rules)

The Information Technology Act, 2000 in India regulates digital communication, transactions, data protection, and cybercrimes. It also covers deceptive patterns. The Act ensures that companies need user consent for collecting sensitive personal data, giving users control.

WHAT ARE THE EFFORTS HAPPENING ON A GLOBAL SCALE TO FIGHT AGAINST DARK PATTERNS?

The United Kingdom of Great Britain and Northern Ireland

The U.K.’s Competition and Markets Authority (CMA)²⁷ is tackling pressure-selling techniques that break consumer protection laws. In 2019, guidelines were released to stop manipulative tactics that influence young users' privacy settings. These guidelines became enforceable under the Data Protection Act, 2018.

The European Union (EU)

The EU Digital Services Act, 2022 bans online platforms from tricking or manipulating users and makes it easier for them to make informed decisions. Companies violating these rules could face fines up to 6% of their global revenue or temporary service suspension. The EU Protection Board's guidelines²⁸ on "dark patterns" help designers and users follow GDPR²⁹ (General Data Protection Regulation) rules. They offer practical tips to identify and prevent sneaky patterns that violate GDPR.

²⁷ The CMA is the principal competition regulator in the United Kingdom. It is a government department that works independently to stop businesses from doing things that harm competition & consumer. Their goal is to create a level playing field and protect consumer from anti-deceptive practices.

²⁸ European Data Protection Board, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them Version 1.0.* (2022), https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (last visited on Jan 23, 2024).

²⁹ The European Parliament and The Council of the European Union, *General Data Protection Regulation*. [online] (Apr. 27, 2016), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (last visited on Jan 23, 2024).

The United States of America

California (a western U.S. State) recently updated the Consumer Privacy Act to tackle sneaky patterns that hinder privacy rights. The law states that consent obtained through deceptive patterns won't be valid. The FTC³⁰ enforces advertising laws related to dark patterns and a recent report showed an increase in sophisticated deceptive tactics. There are laws like the DETOUR (The Deceptive Experiences to Online Users Reduction) Act proposed in July 2023 to combat dark patterns. The Bureau of Consumer Protection has policies to prevent tricky opt-outs and misleading offers. Laws like the CFPA (the Consumer Financial Protection Act), Section 5 of the FTC Act³¹, ROSCA (the Restore Online Shoppers' Confidence Act), EFTA (The Electronic Fund Transfer Act), and TSR (the Telemarketing Sales Rule) protect users from unfair or deceptive marketing practices.

*Federal Trade Commission, Plaintiff, v. LendingClub Corporation, doing business as Lending Club, Defendant.*³²

In this case, the FTC gave back \$10 million to consumers charged unexpected loan fees. Lending Club hid fees with sneaky tactics like tooltip buttons and less noticeable text. Some websites add extra products or hide information until after a purchase.

*Federal Trade Commission, Plaintiff, v. Age of Learning, Inc., a corporation, also d/b/a ABCmouse and ABCmouse.com, Defendant*³³.

In this case, they had a misleading design called a "roach motel." When users tried to cancel subscriptions, they were led through multiple pages of promotions, making it difficult to cancel as promised.

EFFECTIVE STRATEGIES AND RECOMMENDATIONS TO COMBAT DARK PATTERNS

³⁰ The Federal Trade Commission is an independent US Government agency that enforces antitrust laws and protects consumers from deceptive practices and promotes fair competition. It was established in 1914.

³¹ *The Federal Trade Commission Act Section 5: Unfair or Deceptive Practices Background, n.d.*, available at <https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf> (last visited on Jan 23, 2024).

³² Fed. Trade Comm'n v. LendingClub Corp., Case No.18-cv-02454-JSC (N.D. Cal. Jun. 1, 2020)

³³ Federal Trade Commission, Plaintiff, v. Age of Learning, Inc., a corporation, also d/b/a ABCmouse and ABCmouse.com, Defendant Case No. 2:20-cv-7996 (United States District Court Central District Of California, 2020).

A plethora of potential strategies and techniques exist to counteract the deceptive design practices:

- 1) *Transparency*: Encourage enterprises to embrace transparency regarding their design decisions and foster the development of industry-wide ethical design standards. By upholding the principle of "*fraus est celare fraudem*," which translates to "fraud is to conceal fraud," companies should refrain from concealing hidden intentions or deceptive practices. Instead, they ought to communicate any potential consequences or risks to users, empowering them to make informed decisions.
- 2) *User Empowerment*: Advocate for accessible mechanisms that allow users to personalize their experiences, exercise control over their data, and readily opt out of certain features or practices.
- 3) *User Education*: Advocate for accessible mechanisms that allow users to personalize their experiences, exercise control over their data, and readily opt out of certain features or practices.
- 4) *Collaboration*: Foster collaboration among businesses, policymakers, and consumer advocacy groups to establish best practices and ethical design guidelines.
- 5) *Strengthen User Consent*: Ensure companies obtain genuine and informed consent from users, making consent requests clear, and comprehensible.
- 6) *User-Focused Design*: Prioritize user experience and well-being by creating intuitive, user-friendly interfaces without manipulative tactics.
- 7) *Independent Auditing*: Advocate for independent audits of companies' design practices to identify and address any potential dark patterns.
- 8) *Consumer Complaint Mechanisms*: Establish easy-to-access channels for users to report instances of dark patterns and seek resolution, helping identify repeat offenders and drive industry change.
- 9) *Public Awareness Campaigns*: Support campaigns that educate consumers about the dark patterns, empowering them to make informed choices and demand ethical practices from companies.

10) Legislation and Regulation: Governments can enact laws and regulations specifically addressing dark patterns, holding companies accountable for their design practices. This can include penalties for using deceptive tactics.

11) Research and innovation: Research and innovation in user experience can create user-friendly technologies, with funding initiatives and collaborations between academia and industry.

Curbing dark patterns globally is a significant challenge. But by implementing these strategies worldwide and working together with governments, industry players, and users, we can make a difference. Collaboration between countries and regulatory bodies is a key to establishing global standards and responsible design practices. Conducting joint research, and coordinating efforts can help address cross-border issues and create a more trustworthy digital environment for everyone.

CONCLUSION

In light of the aforementioned discourse, it becomes apparent that although the Consumer Protection Act, 2019 and the Rules in India do not explicitly delineate the concept of dark patterns, one can plausibly infer that certain stratagems of a manipulative nature may be encompassed within the ambit of the legislative framework. Thus, it can be posited that India's regulatory apparatus partially addresses the issue of dark patterns, albeit without overt acknowledgment of the precise terminology. To wrap it up, dark patterns pose a significant challenge in the digital landscape, deceiving users and undermining their autonomy. However, by raising awareness, implementing user-centric design principles, and advocating for stronger regulations, we can combat these manipulative tactics. It is crucial for businesses, policymakers, and users to work together to create a transparent and ethical online environment. Together, we can empower users and ensure a fair and trustworthy digital experience for all.