ISSN: 3048-8702(O)

LLRJ

LEX LUMEN RESEARCH JOURNAL

VOLUME 2 - ISSUE 2

2025

EDITOR-IN-CHIEF: DR. RAZIT SHARMA,
PUBLISHER: MRS. RACHANA

LEX LUMEN RESEARCH JOURNAL-ISSN:3048-8702
Open Access, Double blind-Peer Reviewed Law Journal, Licensed by-CC BY-NC-SA.
Editor-in-Chief: Prof. (Dr). Razit Sharma, Publisher: Mrs. Rachana

Volume-2, Issue-2 ***Pages: 133-148***

DARK PATTERNS ON DIGITAL PLATFORMS AND THE NEED FOR LEGAL REGULATION IN INDIA

By- **Nikita Karnik**[1]

ABSTRACT

The fast-paced digitisation in India has increased the public's reliance on digital platforms for everyday activities such as shopping, financial transactions, entertainment, and accessing essential services. Alongside this, the deceptive interface designs of platforms known as dark patterns have also become a growing concern. Dark patterns have been formally defined as "any practices or deceptive design patterns using UI/UX interactions on any platform; 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."[2] *Using doctrinal legal research supported by governmental guidelines, regulatory studies, and authoritative survey data, the paper studies how dark patterns cause harm to consumers, market competition, and challenge regulatory frameworks. The study finds that while India has taken initial steps toward regulating dark patterns, significant gaps are still present due to the lack of binding regulations, fragmented regulatory powers, and enforcement issues. The paper concludes by arguing that stronger enforcement strategies will ensure free and informed*

[1] Intern- Lex Lumen Research Journal.
[2] Department of Consumer Affairs (DoCA) *Dark Patterns Buster Hackathon: About Us*. Government of India. Available at: https://doca.gov.in/DarkPatternsBusterHackathon/about-us.php

Volume-2, Issue-2 *Pages: 133-148*

consent, uphold consumer rights, ensuring fairness, integrity and accountability in India's digital developments.

KEYWORDS: Dark patterns, consumer protection, platform interface regulation, consumer autonomy, regulatory gaps.

INTRODUCTION

Background of the Study

In India, there has been a rapid economic and social digital transformation. This change has been stimulated by widespread access to the internet, digitalised services such as Aadhaar and Unified Payments Interface (UPI), and the rapid growth and increase in usage of digital platforms. Today, people mainly use digital platforms for carrying out everyday activities such as shopping, financial transactions, communication, entertainment and accessing public services. As a result, people now depend heavily on digital platforms for even routine and trivial decisions.

At the same time, concerns have grown about how these interfaces can affect user behaviour. Unlike traditional markets, digital platforms can modify and create algorithms that influence user choice. Through features like pop-ups, colours, and layouts, the platforms can subtly prompt users towards certain decisions. While not all platforms misuse features to push users into choices that mainly benefit the platform and genuinely improve user experience, users are often unable to discern the line between user-friendly designs and manipulative practices on the internet. Features intended to simplify decision-making can, in practice, exploit behavioural biases such as fear of missing out or lack of attention. As a result, users may unknowingly consent to unfavourable terms, subscribe to paid services, or share personal data without fully understanding the consequences of their actions.[3] The

[3] Deceptive Patterns – User interfaces designed to trick you (2023) *Deceptive.design*. Available at: https://www.deceptive.design/

Volume-2, Issue-2 *Pages: 133-148*

absence of clear standards and regulations allows certain platforms to prioritise commercial interests over user autonomous decision-making, reinforcing the need for greater legal scrutiny and consumer protection in the digital arena.

This research seeks to examine the effect of dark patterns on digital platforms in India, assess the efficiency of the existing legal standards and emphasise the need for greater legal regulations. The objective of this study is threefold: To understand the nature and effects of dark patterns. To analyse the existing legal frameworks concerning dark patterns. And to highlight the need for stronger legal regulation to prevent deception of users.

UNDERSTANDING DARK PATTERNS

Origin and Definition

The term "dark patterns" was coined by UK-based User Experience (UX) researcher Harry Brignull in 2010 [4]. While there is no universal legal definition, dark patterns, also known as deceptive patterns, are unethical design patterns and strategies that manipulate users into taking actions they don't intend to take. These dark UX patterns deliberately manipulate choices, create confusion or use emotional triggers to nudge users to make decisions they would not make otherwise.[5] But it is important to note that not all persuasive interfaces are a dark pattern; the difference lies in whether they undermine users' personal autonomy or decision-making.

[4] Harry Brignull (2021) *Bringing Dark Patterns to Light* (speech transcript), Medium, 6 June 2021. https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf

[5] Soroka, A. and Murash, S. (2025) *18 Dark Patterns Examples That Manipulate Users (and How to Avoid Them)*, Eleken Blog. Available at: https://www.eleken.co/blog-posts/dark-patterns-examples

Volume-2, Issue-2 *Pages: 133-148*

Types of Dark Patterns

There are 13 types of dark patterns as mentioned in the Guidelines for Prevention and Regulation of Dark Patterns, 2023 [6]:

i. **False Urgency**: This happens when interfaces subtly imply a sense of urgency or scarcity to the users, indicating a time pressure where none exists to prompt rapid and possibly impulsive decisions from the users. This may include showing a false exclusivity and popularity of the product to present its scarcity and create a fear of missing out on the users. E-commerce platforms use designs such as countdown timers with messages such as *"Only 10 minutes left to claim this deal!"* or *"Only 5 seats left at the lowest price deal!"*

ii. **Forced Actions:** Such designs force the user into completing unwanted steps before letting them proceed to avail a service. This may force the user into buying additional products, having to subscribe or mandatorily sign up, or share personal information to receive a product or service from the platform. Some websites may club newsletter sign-ups with terms and conditions, giving users no option to proceed otherwise, and it can also coerce the user into downloading or visiting an unintended app or website to avail a service. The users might also have to pay additional costs to continue with a service they have already paid for. Such interfaces pop up a *"Sign in"* box to open a website or midway through a service provided, seemingly from which the users cannot opt out.

[6] Central Consumer Protection Authority (CCPA) (2023) *Guidelines for Prevention and Regulation of Dark Patterns, 2023*. Government of India. https://doca.gov.in/ccpa/files/The%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns,%202023_1732707717.pdf

Volume-2, Issue-2 *Pages: 133-148*

iii. **Basket sneaking:** This means the inclusion of additional purchases without the clear consent of the user. This may include adding extra items to the user's cart in e-shopping models without their knowledge, additional services, or extra payments in the name of charity at the time of checkout and purchasing, to which the user cannot opt out. This can be hidden through the term "*necessary fees/service fees*" such as delivery charges, gift wrapping charges, additional subscription plans, or charging extra taxes over the taxes charged by the government. Platforms can also preselect default products or services that are either the most expensive or unfavourable without the user's input

iv. **Subscription trap:** This can include making it difficult or impossible to cancel a subscription, making the cancellation or account deletion option hard to find in the interface. This can also include automatically transitioning users from a free trial period subscription to a paid subscription without a proper notice of the end of the free trial or a cancellation option available at the end of the trial period. A cumbersome, confusing and complex cancellation or account deletion process dissuades the user from terminating a service as per their choice.

v. **Confirm shaming:** Platforms may guilt-trip the users into an unwanted choice through guilt-laden language, phrases, emotional videos, and images that create an emotion of guilt, shame by subtly ridiculing the user for opting out of fees such as donations, subscription or insurance plans. Some examples include health websites that may prompt the users by stating *"No thanks, I don't care about my health"* when the user declines a subscription or insurance plan, or instances when a user declines donating to a cause and is shown with pop-ups such as *"No, I don't care about starving children."*

Volume-2, Issue-2 *Pages: 133-148*

vi. **Drip Pricing:** It is the practice where hidden or additional fees are revealed only at the checkout, such as a charging a higher amount than the one disclosed at the time of purchase, products or services can also be falsely advertised as free of charge with vague or no disclosure that to continue availing a service or avail the complete service the user might have to pay additional charges. Examples include where consumers might have to pay "*rain fees*" or "*small cart fees*", which are revealed only at the time of checkout.

vii. **Disguised advertisements:** Some platforms have disguised advertisements that blend or get hidden with the genuine interface features, tricking the users into engaging with them, such as clickable pop-ups that lead to another website from the ad, for example some platforms might have a fake download button which the users might click because they believe the button would download their intended file but it instead redirects to advertisements or malware, the same works with the "*X*" button which the users click believing it will close a certain ad or pop-up. Some websites can blur the line between the actual content and ads, or the entire website background is sensitive to clicks, and clicking anywhere opens an ad or redirects to a new tab.

viii. **Bait and Switch:** This occurs when users are promised one outcome but receive something different. This can happen in instances where users click the close button for a site or updates window, hoping to close or terminate a window, but instead trigger the update process. Some products may also be advertised as available to consumers during the shopping process, but when they reach the checkout, the product is shown as sold out, and they are prompted to buy a more expensive version of the product instead. A service may also be offered as a free product after a mandatory sign-up

Volume-2, Issue-2 *Pages: 133-148*

process, but after the user completes it, the product requires payments, leading to the user unwillingly disclosing their personal data.

ix. **Interface Interference:** This means the use of poor design elements that manipulate the interface with elements such as low contrast, obscure placement of the feature that hides the actual information or highlights only certain information, which can misguide the user into taking undesirable actions. This can manifest in ways such as platforms designing the close button in a lighter colour or using a smaller font for cancellation options, or using opposite colours as normally used and understood, such as using green colour for "*No*" and red colour for "*Yes*" if the website is asking whether the user wishes to cancel a certain service.

x. **Nagging:** This practice entails persistent prompts that repeatedly interrupt the user experience in the form of requests, options, ads, information or clickable prompts, such as requests to turn on notification or a pop-up for cookies with no option for declining, the users also may get bombarded with pop-ups to subscribe to premium plans or newsletters during their use of the service, such requests usually only have the option of "*Not now*" or "*Maybe later*" ensuring that the prompt will reappear later whether the user likes it or not.

xi. **Rogue Malware:** It involves using deceptive designs such as fake virus alerts where pop-ups mislead the user by showing warnings that the device is infected with a virus, which is actually malware or a tool requiring payment with fake and malicious download buttons and clickjacking which means an overlay of misleading elements, the user might click the "*Play*" button on a video but they might end up authorising the installation of rogue software.

xii. **Trick question:** Platforms may intentionally use ambiguous language or phrases to trick users into unintended actions. For example, subscription

Volume-2, Issue-2 *Pages: 133-148*

prompts might display phrases like "*You will receive updates about products you may like unless you click to opt out.*" This can confuse users about whether to check the prompt box for their desired service.

xiii. **Saas billing:** This is a technique used to deceptively extract payments, such as hidden auto-renewals, a difficult cancellation process and hidden costs in a Software as a Service (SaaS) business model. This may include charging users for a trial without notice, forcing credit card information for free access to a service and making it easy to sign up but deliberately making it difficult to cancel, with features such as hiding the cancellation option, making it difficult to find in the settings or requiring a phone call, a message, or an email to cancel the subscription or account.

THE HARMFUL EFFECTS OF DARK PATTERNS

Dark patterns have a significant impact on users; they are not just harmless design features. They have detrimental effects on the users, market competition and consumer trust in the digital system.

Consumer Consent and Privacy

Dark patterns undermine the ethical principle of informed consent important for protecting consumer rights and privacy. When users are misled, subtly nudged or coerced through interface designs, leading them to share personal data unintentionally, pay for a subscription or reluctantly incur financial costs. This also violates the personal data protection policy and consent-based regulation to protect

Volume-2, Issue-2 *Pages: 133-148*

data through clear, specific and informed consent of the users as emphasised in the Digital Personal Data Protection Act, 2023.[7]

Financial Harm to the Consumers

One of the most common sources of financial harm arises from drip pricing and hidden costs. In such cases, additional charges are disclosed at the checkout when users have already invested considerable time and energy in purchasing and choosing the products, thus they may have no choice but to proceed despite the increased costs to avoid feeling wasteful of their time and efforts, a phenomenon known as the "*sunk cost fallacy*."[8] Such payments can exceed the consumer's initial expectations and budget and lead to higher financial costs and burden over time. Such practices strategically extract monetary value from consumers rather than enable fair market practices. From a legal perspective, this is concerning because it involves free and fair market practices and consumer choice and freedom at stake, thus reiterating the need for stronger regulation to avoid financial exploitation of consumers.

Market Competition and Ethical Issues

In a research study conducted by the *Advertising Standards Council of India (ASCI)* [9] in 2024, it was found that 52/53 apps studied exhibited at least 1 Deceptive Pattern, with Privacy Deception being the most common, with 79% of the studied apps involving it. The study observed 100% instances of Confirm Shaming by Travel Booking platforms, while the highest instances of dark patterns were observed in the activities

[7] Ministry of Electronics and Information Technology (MeitY) (2024) Digital Personal Data Protection Act, 2023. Government of India. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[8] Veronika Tait and Harold L. Miller Jr (2019) *Loss Aversion as a Potential Factor in the Sunk-Cost Fallacy*, *International Journal of Psychological Research* 12(2): 8–16. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7318389/

[9] Veronika Tait and Harold L. Miller Jr (2019) *Loss Aversion as a Potential Factor in the Sunk-Cost Fallacy*, *International Journal of Psychological Research* 12(2): 8–16. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7318389/

Volume-2, Issue-2 *Pages: 133-148*

involving purchasing, booking or subscribing. Along with this, 9/9 e-commerce apps were shown to make it difficult for users to delete their accounts, and 4/5 health apps relied on False urgency to pressure or rush users into making decisions. While the study does not speak for every platform and its practices across India, it is nonetheless significant. The consistency with which deceptive patterns appear across sectors shows that this might be a systemic design tendency rather than an isolated practice. This raises concerns about ethical risks where consumer welfare and rights seem secondary to profit-making practices, weakening integrity and eroding consumer trust. Platforms can use these techniques to also gain an unfair advantage over competitors by manipulating the users.

PRESENT LEGAL FRAMEWORK TO ADDRESS DECEPTIVE PATTERNS

Consumer Protection Act, 2019[10]

India has made the use of dark patterns illegal under the Guidelines for Prevention and Regulation of Dark Patterns, 2023, classifying them as unfair trade practices under the Consumer Protection Act, 2019. The Central Consumer Protection Authority (CCPA) mandated self-audits for e-commerce platforms to eliminate these practices in June 2025, with the compliance deadline passing in September 2025[11]. However, these guidelines are broad, non-binding and lack a clear regulatory process, leaving the enforcement upon the discretion of authorities.

[10] Government of India, The Consumer Protection Act, 2019 (Act No. 35 of 2019) (9 Aug. 2019). Available at: https://ncdrc.nic.in/bare_acts/CPA2019.pdf

[11] Central Consumer Protection Authority (CCPA) (2025) *Advisory on Self-Audit by E-Commerce Platforms for detecting the Dark Patterns on their platforms*, Department of Consumer Affairs, Government of India. Available at: https://doca.gov.in/ccpa/files/Advisory-7.pdf

Volume-2, Issue-2 *Pages: 133-148*

Information Technology Act, 2000[12]

The IT Act was originally created to regulate digital intermediaries' obligations, due diligence, and content takedown systems. It addresses cybersecurity and e-commerce in order to protect personal data and punish its misuse, but it does not directly address dark patterns. This vacuum had allowed dark practices to continue without legal restrictions. While not specifically for deceptive patterns, the IT Act can regulate platform conduct to prevent harm to users.

Digital Personal Data Protection Act, 2023[13]

The DPDP Act can directly counter dark patterns that involve manipulating user consent for personal data. It requires consent to be free, specific, informed, unconditional, and unambiguous, and highlights that taking consent back should be as easy as giving it. However, specified and direct provision on dark patterns can weaken its enforceability and ability to penalise violations.

E-Commerce Rules and Self-Regulation Guidelines

India's *Consumer Protection (E-Commerce) Rules, 2020* [14] require transparent disclosure of prices, refund policies, and terms, which means that deceptive patterns such as drip pricing directly contradict these rules, yet their enforcement remains vague. Self-regulation has been mandated by the CCPA, the self-audit deadline of 3 months has also passed, yet users are still facing issues with deceptive patterns such as drip pricing, false urgency, pushing them towards impulse purchases and disclosing

[12] Government of India, Information Technology Act, 2000 (Act No. 21 of 2000) (9 Jun. 2000). Available at: https://www.meity.gov.in/static/uploads/2024/03/IT-Act-Rules_2000_0.pdf
[13] Ministry of Electronics and Information Technology (MeitY) (2024) Digital Personal Data Protection Act, 2023. Government of India. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
[14] Ministry of Consumer Affairs, Food and Public Distribution (2020) *Consumer Protection (E-Commerce) Rules, 2020*. Government of India. Available at: https://consumeraffairs.gov.in/public/upload/files/E%20commerce%20rules_1732703966.pdf

Volume-2, Issue-2 *Pages: 133-148*

personal information. The consumer affairs ministry has also taken notice of such dark practices, with the Consumer Affairs Minister affirming that platforms that charge an extra fee for cash on delivery will now face action against them after a probe into such practices.[15]

REGULATORY GAPS IN THE INDIAN LEGAL FRAMEWORK

Consent-based Focus

Indian legal regulations heavily rely on the principle that if the user was informed and still consented to a feature, it is a valid consent. While the principle in itself is not an issue, deceptive patterns directly undermine the effectiveness of users' choices by manipulating their decisions or urging them towards impulsive, uninformed decision-making. When consent is gotten through the manipulation of interface designs, the legal assumption of informed consent becomes questionable.[16] Yet, current legislation does not clearly address whether consent obtained through dark patterns is invalid, creating uncertainty for its effective enforcement and compliance.

Multiple Regulating Authorities

The responsibility for regulating digital platforms is dispersed across multiple authorities, such as:

- Central Consumer Protection Authority (CCPA)
- Ministry of Electronics and Information Technology (MeitY)
- Authorities for specific sectors, such as the RBI for fintech

[15] NDTV (2024) *Extra fee for cash on delivery: Minister Pralhad Joshi promises crackdown on dark patterns*. Available at: https://www.ndtv.com/india-news/pralhad-joshi-cod-extra-fee-for-cash-on-delivery-minister-promises-crackdown-on-dark-patterns-9392631

[16] DPO India (2024) *Consent management in India under the Digital Personal Data Protection Act*. Available at: https://www.dpo-india.com/Blogs/consent-management-india-dpdp-act/

Volume-2, Issue-2 *Pages: 133-148*

This dispersion of regulatory power can result in overlapping jurisdictions and regulatory blind spots, particularly where dark patterns create issues in consumer protection, data protection, and financial regulation.

Enforcement Constraints

Even with the existing legal framework or a possibility of a sturdier legal framework in the future, there may still be some gaps in enforcing those laws, such as:

i. **Low consumer awareness** – Many users are unaware that deceptive practices may be legally questionable, resulting in under-reporting. More importantly, many users still do not know what dark patterns are on digital platforms and cannot discern between genuine interface designs and deception.[17]

ii. **Reactive enforcement** – Regulatory action typically follows consumer complaints rather than proactive audits; thus, without consumers reporting and having knowledge about dark patterns, it is difficult for legal action to be taken.

iii. **Resource and capacity constraints** – Regulatory authorities face capacity and resource limitations in auditing complex digital interfaces across thousands of platforms in India; a comprehensive audit is thus difficult to undertake, and the integrity of self-audits by the digital platforms is still questionable.

iv. **Ambiguity in standards** – Without statutory definite standards, determining what constitutes a prohibited dark pattern remains subjective, thus even its enforcement becomes subjective and cannot be standardised easily.

THE NEED FOR COMPREHENSIVE LEGAL REGULATIONS IN INDIA

[17] '*Manipulation under the click: Unravelling dark patterns in digital consumerism and legal countermeasures in India*', *Manupatra Articles*. Available at: https://articles.manupatra.com/article-details/Manipulation-Under-The-Click-Unravelling-Dark-Patterns-In-Digital-Consumerism-And-Legal-Countermeasures-In-India

Volume-2, Issue-2 *Pages: 133-148*

Limitations of Self-Correction in the Market

A common argument against strict regulation is that consumer choice and competition eventually discourage unfair practices. Theoretically, users can avoid platforms that engage in dark patterns, but in practice, this is not always possible. This is because normal users lack the information, awareness, or authority needed to identify and penalise such practices.[18] On many platforms that operate in smaller sectors of the markets, users have limited choices, making it difficult to opt out of their services even if deception is recognised.

Consumer protection

Vulnerable groups of consumers, such as the elderly, children or illiterate people, need stronger protection against dark patterns as they are more likely to get trapped in such manipulative patterns. In India, regulation is particularly important due to different levels of digital literacy and the heavy reliance on platforms for everyday and essential services. Legal systems thus need to act as a preventive and corrective tool to ensure fairness, transparency and accountability of digital platforms.[19]

Lack of Explicit and Binding Regulations

Present consumer protection laws mostly address misleading practices, such as false representation or unfair contract terms. However, dark patterns work at the level of interface design and shape user choices before any clear misrepresentation occurs. This makes them difficult to address under existing legal frameworks. There have been guidelines for self-auditing dark patterns, but it has been largely non-binding, thus difficult to enforce. There needs to be binding regulations and laws for

[18] Luguri, J. & Strahilevitz, L.J. (2021) *Shining a Light on Dark Patterns*, Journal of Legal Analysis, 13(1), pp. 43–109. Available at: https://academic.oup.com/jla/article/13/1/43/6180579

[19] Centre for Digital Public Policy (CDPP) (n.d.) *The need for the triangular approach – dark patterns*. Available at: https://www.cdpp.co.in/articles/the-need-for-the-triangular-approach---dark-patterns

Volume-2, Issue-2 *Pages: 133-148*

preventing and penalising deceptive patterns that undermine informed consent and freedom of choice. Along with this, it is important to ensure that such regulations do not penalise platforms for using honest, persuasive interface models but instead differentiate between genuine persuasive from harmful manipulation of the users, upholding consumers' rights.

RECOMMENDATIONS

Based on the study, the following reforms are proposed:

Mandatory Design Audits

Regulating authorities should be mandated to conduct periodic interface audits for platforms, particularly in sectors involving financial commitments or sensitive data.

Revised Standards for Consent

Data protection regulations should explicitly recognise that consent obtained through a manipulative design is invalid.

Stronger Enforcement Powers to Authorities

- Compliance and enforcement from prevention of dark patterns should be made binding.
- Power to issue binding orders to correct interface designs after auditing.
- Regulators should have the authority to impose proportionate legal penalties.

Initiatives for Consumer Awareness

The government can initiate digital literacy campaigns that educate users about common dark patterns and provide appropriate redressal forums for users to report the usage of deceptive patterns.

CONCLUSION

Volume-2, Issue-2 *Pages: 133-148*

Dark patterns represent an important and evolving challenge in India's digital economy. While existing legal frameworks do offer partial protection, they are still insufficient to address the specific nature of deceptive interface designs. This research thus emphasises that explicit legal regulation of dark patterns is not only useful but necessary to safeguard consumer rights, personal choice and data, maintain market fairness, and uphold the integrity of digital consent. Clear and proactive legal regulations can help India ensure that its digital platforms remain inclusive, ethical and respectful of consumers' wellbeing and rights.