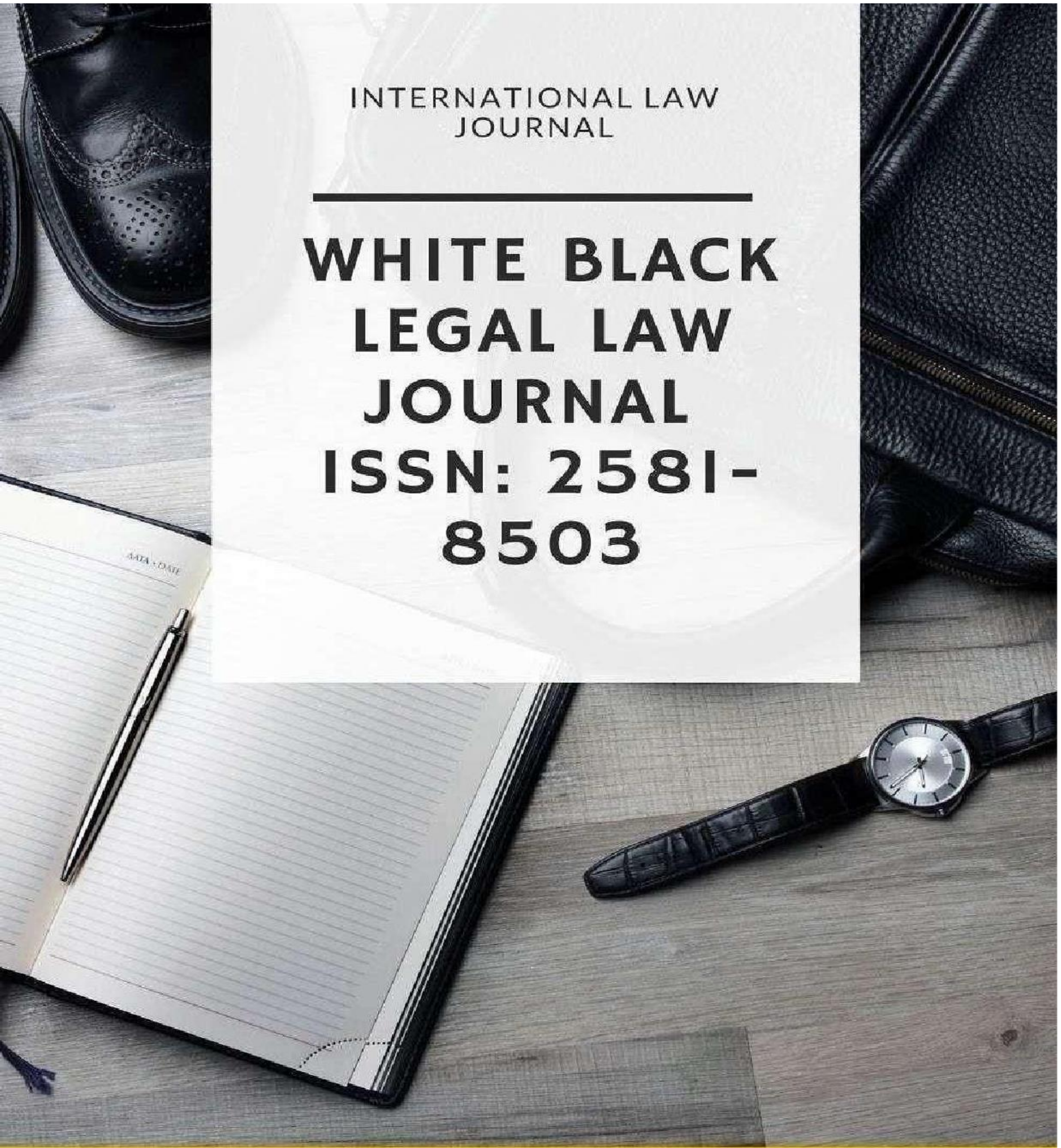


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

 ISSN: 2581-8503

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

Volume 4 Issue 1 | Sep 2026 ISSN: 2581-8503

DARK PATTERNS AND PSYCHOLOGICAL MANIPULATION IN ONLINE SHOPPING: A LEGAL ANALYSIS

AUTHORED BY – HARIHARAN & ANESHA V

INDEX

S.NO	PARTICULARS
1.	DIVISION OF PARTICIPATION
2.	BACKGROUND OF STUDY
3.	STATEMENT OF RESEARCH PROBLEM
4.	RESEARCH METHODOLOGY
5.	RESEARCH QUESTIONS
6.	LITERATURE REVIEW
7.	DARK PATTERNS UNDER ANNEXURE I OF THE CCPA GUIDELINES (2023)
8.	FOREIGN LAW AND ITS IMPLICATIONS ON DARK PATTERNS
9.	INDIAN PERSPECTIVE ON REGULATION OF DARK PATTERNS
10.	PSYCHOLOGICAL IMPACT OF DARK PATTERNS
11.	RECOMMENDATIONS
12.	CONCLUSION
13.	BIBLIOGRAPHY
14.	AI AND PLAGIARISM REPORT

BACKGROUND OF STUDY

What seems like a choice on your screen might really be a trick coded in.

The online shopping world has changed how people buy things. But with new ideas came sneaky tricks called dark patterns.

"When tricks take over, the shopping cart turns into a trap."

These design tricks include timers that rush you, hidden fees that pop up at the end, and fake shortages that make you think items are running out. They go beyond smart ads. They push people using mind games, taking away real choices and fair deals.

This study looks closely at the legal side of these tricks. It fits them into rules for consumer rights. The work checks how dark patterns mix tech, human thoughts, and business. It studies effects under India's laws and global ones. It points out weak spots in rules and checks. Using court cases, rule books, and looks at other countries' laws, this paper says dark patterns are more than bad tricks. They are new ways of unfair online trade. The study suggests a plan based on rights. It balances new ideas with respect for buyers. It calls for rule changes to stop tricks without hurting honest business. In the end, this work shows how laws need to change for online sales. It aims to keep shopping as a place of real choices, not forced ones. "In online sales, the worst scams aren't breaking laws. They hide in the design."

You feel uneasy leaving items in your online cart. Or you hesitate to close an ad for a "special" deal. These feelings aren't by chance. They aren't harmless. They come from planned digital tricks known as dark patterns.

Dark patterns are design methods in apps and sites. They guide users to act in ways they wouldn't normally. They use mind triggers to help companies over users.

Harry Brignull first named "dark patterns." He called them tricks in websites and apps that make you do things like buy or sign up without meaning to. These designs hide real options. They lead users to set paths.

On November 30, 2023, India's Central Consumer Protection Authority issued rules to stop and control dark patterns. These are the first such rules in India. Clause 2(e) defines dark patterns. Annexure 1 lists 13 types with examples: false urgency, basket sneaking, confirm shaming, forced action, subscription traps, interface interference, bait and switch, drip pricing, disguised ads, nagging, trick questions, SaaS billing, and rogue malware.

These new rules build on the Advertising Standards Council of India's guidelines from June 2023. Those covered four types. The new ones add many more. This step boosts buyer safety. It sets an example for other places.

A 2019 Princeton report checked nearly 11,000 shopping sites. It found 11% used misleading, pushy, or illegal tricks. Still, dark patterns are on the rise. A late 2023 report in the National Law Review noted this, based on U.S. Federal data.

STATEMENT OF RESEARCH PROBLEM

Online spaces for shoppers now often use clever design tricks. These tricks play on mental shortcuts and biases in the mind. Experts call these "dark patterns." They push people to do things they might skip, like signing up by mistake, spending too much, or sharing private details. Though hard to spot, dark patterns harm user control, privacy, and faith in web shopping. Around the world, rule-makers see the risks. But their rules differ in reach and follow-through. In India, the Central Consumer Protection Authority put out rules in 2023 to stop and control dark patterns. This marks the first real set of laws on the issue. It builds on past self-made rules from the Advertising Standards Council of India.

The rules list tricky actions. Yet they fail to tackle the mind factors that leave users open to tricks. Things like fear of loss, rush from scarcity, or following the crowd make people easy targets. Enforcing these rules proves tough. Online sales cross borders. Platforms change fast too. No one knows yet how these rules fit with old laws on buyer rights, data safety, and ads. These weak spots spark big doubts. Do India's rules work well? Are they strong for the long run?

This study asks if India's current rules shield buyers from dark patterns. Or do we need more steps? Legal ones, tech tools, and teaching could help build a fair, open, and honest online market.

RESEARCH METHODOLOGY

This study uses a doctrinal and qualitative method. It combines detailed legal review with a comparison of top global practices. Key sources of primary data are laws like the Consumer Protection Act of 2019 and the Information Technology Act of 2000. They also include recent rules, such as the IT Intermediary Guidelines and Digital Media Ethics Rules of 2021.

Secondary data comes from court cases, reports from regulators, scholarly papers, and legal decisions in India and abroad.

The work starts with sorting dark pattern methods. It draws from books and reviews of online platforms. Next comes a close look at how these methods fit with rules on consumer rights. Talks with experts and a review of those involved add to the main research. The goal is to spot weak areas and propose changes to laws.

RESEARCH QUESTIONS

1. How well do the CCPA Guidelines of 2023 control dark patterns in India? How do they stack up against world laws on tricky design tricks?
2. In which ways do the CCPA Guidelines match or differ from rules in places like the European Union (Digital Services Act and GDPR), the United States (FTC Act and
3. ROSCA), and the United Kingdom (Consumer Protection from Unfair Trading Regulations)?
4. What can India learn from top global ways to make its rules stronger against dark patterns?
5. How does India's ability to enforce rules compare to models used around the world to stop harmful digital designs?

LITERATURE REVIEW

Dark patterns—designs in the user interface and experience of websites and applications that influence, manipulate, or trap users into taking actions they would not otherwise perform—have been theorised by interdisciplinary scholars for more than a decade. It was popularised by Bring and is now formally considered by both HCI and security/privacy researchers who demonstrate how design decisions (wording, layout etc.) can systematically undermine user autonomy, potentially leading to measurable harms such as unsolicited purchasing behaviour, involuntary data disclosure, and subscription trap expansion. Empirical research has both categorised "dark pattern" apart from other common pattern types and verified their pervasiveness across massive numbers of websites and applications, positioning dark patterns as a repeatable, scalable phenomenon rather than one-off design mistakes.

Expanding on the conceptual taxonomies, recent work has addressed detection, measurement and harms of dark patterns. While there have been significant large-scale crawls and annotation efforts documenting recurring varieties (e.g., nagging, confirm-shaming, bait-and switch, hidden costs, interface interference) and methodologies – both manual coding solutions and automated heuristics — to systematically detect them at scale. More recent synthesis reviews further note methodological limitations, specifically the variation in the terms and definitions used across datasets, the challenges of automated detection when exposure patterns are context specific, and insufficient attention to differences based on jurisdiction as to how harms

 ISSN: 2581-8503

manifest. These empirical traditions offer the vocabulary and technology for policy makers and auditors to map out problematic interfaces in a more methodical fashion.

There is an increased regulatory focus in India – for instance, with the promulgation of the Central Consumer Protection Authority's "Guidelines for Prevention and Regulation of Dark Patterns, 2023", which define dark patterns (and what comprises to such behaviour), provide examples and state that consumer-law remedies are applicable to conditions that lead a user to make a decision she otherwise would not have made; the guidelines cover platforms, advertisers and sellers (including foreign entities targeting Indian consumers), thereby taking an extraterritorial approach. The CCPA has continued with compliance nudges, issuing advisory guidelines to e-commerce platforms to perform self-audits to identify and remove dark patterns, indicating a willingness to pivot from advice giving toward oversight. These are indeed concrete departures from the Indian regulatory doctrine to consider deign practices as being unfair trade practices and not merely ethics figures.

Observers have pointed out that India's dark-pattern regulation is not "standalone" (independent) as it meets at the points of the Information Technology Act regime and intermediary due-diligence rules, which impose compliance responsibilities on platform intermediaries, and with data-protection law – specifically the mandatory Digital Personal Data Protection framework anchored in free and informed consent. This multi-layered regulatory environment is both opportunity and recipe for complexity: on the one hand, it enables dark-pattern anxieties to be channeled through a number of legal pathways (consumer redress, data-protection enforcement, intermediary liability); but it also raises issues of jurisdictional overlap and coordination among enforcements authorities as well as unclear thresholds under law when design choices are borderline persuasive rather than straightforwardly deceptive.

Given regulatory advancements, the literature discerns remaining challenges and omissions for you to fill. First, definitional variance and context-sensitivity make enforcement of bright lines hard —what is manipulative in one situation might be appropriate persuasive design in another. Second, current detection methods fail to capture subtle patterns that emerge based on temporal or multimodal cues (e.g., microcopy + timing). Third, regulatory overlaps in consumer law, cyber law, intermediary rules and data-protection statutes necessitate institutional coordination mechanisms that are still immature in India; recent advisories vacillate towards audits but there is scarce evidence on the result from enforcement. Finally, we should seek for normative work to connect identifiable dark patterns to quantified harms (economic, privacy or autonomy) so regulatory responses can scale outcome-oriented remedies and sanctions accordingly. These lacunae suggest rich grounds for empirical work, doctrinal analysis and design-law research of a sort that includes development of Indian context detection rubrics, comparative legal studies on enforcement paths, and proposals for institutional coordination and proportional remedy.

DARK PATTERNS UNDER ANNEXURE I OF THE CCPA GUIDELINES (2023)

The Guidelines issued by the Central Consumer Protection Authority (CCPA) formally acknowledge thirteen types of dark patterns. Each type represents a manipulative design strategy aimed at exploiting consumer behaviour, often leveraging cognitive biases or information asymmetry.

a. FALSE URGENCY

False urgency is a dark pattern that influences consumers by creating or exaggerating a sense of scarcity or time pressure, encouraging hasty decisions that they might not otherwise make. This tactic often manifests through mechanisms such as fake countdown timers, misleading claims like "only 1 left in stock," or deceptive popularity alerts such as "20 people are viewing this right now." These strategies exploit psychological tendencies such as scarcity bias and fear of missing out (FOMO). While these methods may enhance sales, they undermine consumer autonomy, privacy, and trust. Recognizing its detrimental impact, the CCPA Guidelines of 2023 in India explicitly classify false urgency as a prohibited dark pattern, mandating that any claims regarding urgency or scarcity must be accurate and verifiable. This provision aims to mitigate manipulative practices that distort consumer choice and promote greater transparency in digital marketplaces.

b. BASKET SNEAKING

Basket sneaking refers to a manipulative digital practice in which additional items, services, or charges are included in a user's shopping cart without their explicit consent, thereby increasing the total payable amount without the consumer's awareness. This may involve automatic inclusion of products, add-on services, or even charitable donations through pre-checked options at checkout. For instance, a movie ticket booking platform that automatically checks a ₹1 donation box without informing the user exemplifies basket sneaking. The Guidelines specify that legitimate charges, such as delivery fees, applicable taxes, or optional services that are clearly disclosed, do not fall within this category, as they are necessary, transparent, and consented to. Basket sneaking undermines consumer autonomy by subtly pressuring users into paying for items they may not desire, representing a deceptive digital strategy aimed at increasing revenue at the consumer's expense.

c. CONFIRM SHAMING

Confirm shaming is a dark pattern that employs emotions such as guilt, fear, shame, or ridicule to sway consumer decisions. By framing a user's refusal in negative or emotionally charged terms, businesses exert pressure on individuals to take actions they might not otherwise choose. For example, when a travel booking platform prompts users with a message like "I will stay unsecured" if they decline insurance, it implicitly shames the user for not opting in. Similarly, subscription services might use phrases such as "No, I don't want to save money" or "I prefer to miss out on this offer," fostering a sense of personal inadequacy or regret. This technique capitalises on emotional vulnerability, nudging consumers toward compliance for the commercial benefit of the entity while undermining informed and voluntary decision-making.

d. FORCED ACTION

Forced action is a dark pattern wherein users are compelled to undertake additional or unrelated actions as a prerequisite to accessing the product or service they originally sought.

This may involve requiring subscription to a newsletter, providing personal or sensitive information, downloading additional software, or purchasing supplementary goods or services. For instance, a health and wellness website might mandate completing a newsletter subscription before allowing the purchase of a supplement. By linking access to unrelated obligations, such practices compromise consumer autonomy, restrict genuine choice, and manipulate behaviour for commercial gain, effectively transforming voluntary decisions into coerced compliance. Forced action is particularly insidious as it disguises exploitation as a standard procedural requirement, pressuring users to comply under the guise of necessity.

e. SUBSCRIPTION TRAP

A subscription trap is a manipulative digital practice where users are subtly pressured into maintaining a subscription or service by making cancellation intentionally challenging, confusing, or time-consuming. Platforms employing this dark pattern may obscure the cancellation option deep within menus, necessitate lengthy interactions with customer support, or require the provision of payment details even for "free" trials that automatically convert into paid subscriptions. For example, a streaming service may facilitate easy online subscriptions while mandating that cancellations can only be processed via a phone call, thereby creating unnecessary friction. This pattern exploits consumers' tendencies to avoid effort, effectively locking them into recurring payments. By complicating the exit process, subscription traps undermine informed consent, erode user autonomy, and extract revenue under the pretext of standard subscription procedures.

f. INTERFACE INTERFERENCE

Interface interference is a dark pattern that manipulates the visual design of digital interfaces to subtly influence user behaviour and guide them toward specific actions, often contrary to their true preferences. This manipulation can involve emphasising certain options while downplaying or obscuring others, creating a visual hierarchy that nudges users toward the choice favoured by the platform. For instance, a pop-up might display the "Yes" button in bold, bright colours and a prominent position, while the "No" button is small, greyed out, or positioned inconspicuously. Such deliberate asymmetry exploits cognitive shortcuts, increasing the likelihood that users will select the highlighted option without fully considering alternatives. By shaping perception through design rather than providing neutral information, interface interference undermines informed decision-making and compromises consumer autonomy in digital environments.

g. BAIT AND SWITCH

Bait and switch is a deceptive digital strategy wherein users are initially attracted by an appealing offer or product, only to find that the promised item is unavailable or replaced with a less favourable alternative, often at a higher cost, upon attempting to complete the transaction. For instance, an e-commerce platform might advertise a premium gadget at a significant discount to draw clicks, only to inform the consumer at checkout that the item is "out of stock" and offer a more expensive substitute instead. This practice exploits consumer expectations and cognitive biases, such as the sunk-cost fallacy, compelling users to accept the substitute after investing time or effort in the purchasing process. By creating false initial incentives, bait and switch manipulates decision-making, erodes trust, and coerces consumers into transactions they may not have voluntarily chosen.

h. DRIP PRICING

Drip pricing is a manipulative practice in which the complete cost of a product or service is not transparently presented upfront, with additional fees, charges, or conditions revealed progressively during the purchase process. This tactic is designed to obscure the true price and encourage commitment before users are fully aware of the total expense. For example, an airline may advertise a low base fare to attract bookings, but subsequently disclose baggage fees, convenience charges, service taxes, or seat selection costs at later stages of the checkout process. Similarly, e-commerce platforms may require the purchase of supplementary items or services to access a deal that initially appeared free or low-cost. By withholding complete pricing information, drip pricing limits consumers' ability to make informed comparisons, exploits impulsive decision-making, and undermines transparency, ultimately benefiting the seller at the consumer's expense.

i. DISGUISED ADVERTISEMENT

Disguised advertisement is a dark pattern in which promotional content is intentionally crafted to resemble authentic, non-commercial material, misleading users into interacting with it under the impression that it is unbiased or user-generated. This may include paid endorsements presented as news articles, genuine product reviews, blog posts, or social media content that seamlessly blends with organic material. For example, a skincare brand might post a sponsored review that appears to be an independent user testimonial, leading consumers to overestimate its credibility. The CCPA Guidelines clarify that the responsibility for clearly disclosing the promotional nature of such content rests with the advertiser or seller rather than the hosting platform. By camouflaging advertisements, this pattern exploits trust, deceives users, and manipulates decision-making, compromising informed consent and transparency in digital marketplaces.

j. NAGGING

Nagging is a dark pattern characterised by persistent, repetitive, or intrusive prompts designed to coerce action through annoyance or fatigue rather than informed choice. This can manifest as constant pop-ups, repeated push notifications, emails, or in-app reminders that pressure users to download an app, finalise a purchase, or engage with a service. For example, an e-commerce platform may frequently remind a user to complete a shopping cart, while a mobile application might continuously prompt for installation or subscription. By inundating the user with repetitive messaging, nagging exploits cognitive and emotional fatigue, shifting decision-making from deliberate and informed choice to compliance driven by irritation or impatience. This tactic undermines consumer autonomy and manipulates behaviour for commercial gain, presenting a subtle yet effective form of digital coercion.

k. TRICK QUESTION

A trick question is a dark pattern that manipulates users through confusing, ambiguous, or misleading language to steer them toward actions they may not intend to take. This often involves the use of double negatives, complex phrasing, or misleading labels that exploit user inattention or haste. For instance, a pop-up may inquire, "Do you want to cancel your subscription?" with options labeled "Continue" and "Cancel," where selecting "Continue" unintentionally maintains the subscription instead of canceling it. Such design tricks take advantage of cognitive overload and rushed decision-making, effectively coercing users into undesired outcomes. By creating linguistic ambiguity, trick questions undermine informed consent and manipulate consumer behaviour for commercial benefit, representing a subtle yet impactful form of digital deception.

l. SaaS BILLING

SaaS billing is a dark pattern commonly observed in software-as-a-service models, wherein users are deceptively charged for subscription renewals without adequate notice, consent, or clear communication. For example, a free trial may automatically convert into a paid subscription once the trial period concludes, without notifying the user or providing an easy means to opt out. Similarly, recurring charges may persist even after a user believes they have canceled the service. This practice exploits inattention, inertia, and lack of awareness, effectively locking users into payments they did not knowingly agree to. To mitigate this issue, transparency, explicit consent, and timely notifications regarding subscription renewals are essential. In the absence of such safeguards, SaaS billing dark patterns compromise consumer autonomy, violate trust, and constitute a deceptive commercial practice.

m. ROGUE MALWARE

Rogue malware represents one of the most harmful dark patterns, wherein users are deliberately misled into believing that their device is infected with a virus or malware. Fraudulent pop-ups, warnings or alerts claim urgent action is required.

The CCPA Guidelines for Prevention and Regulation of Dark Patterns (2023) mark a significant step forward in protecting digital consumers in India. Guidelines for Prevention and Regulation of Dark Patterns (2023) are a specialised sub-set which works specifically in this area: e-commerce companies' deceptive design strategies, digital advertising and online transactions. These Guidelines Seek to identify and restrict manipulative practices which harm consumer autonomy, choice in using digital marketplaces, or trust in them as well.Especially with few details on how to implement any of them, the Guidelines are the most notable achievement of our national regulation. One concern, however, is that they make clear Deliberations for iterate whether a dark pattern represents an attempt to mislead or manipulate users and provide no objective criteria allowing judges with different ideas of right and wrong this vagueness in the law may lead to inconsistent judgements vital for enforcement Another limitation is that "dark patterns" as defined by these Guidelines is quite broad, leading to potential confusion in categorising new or borderline digital practices. One more highly significant feature that must be noted: there are no statutory penalties associated with violations under this legislation in India. Although the Draft Guidelines contained provisions for imposing sanctions on perpetrators of illegal practices, these were not included at all in the final version–thus curtailing CCPA authority to enforce since although CPA does enable it to take necessary actions for consumer protection. Not only must we consider the original intentions which led to KJF being used as the basis this new set of regulations, but the specific impacts of these Guidelines as well.

To plug these gaps, regulatory authorities and relevant minis- tries would need to join forces with experts to assess how effective it might be to regulate dark patterns in digital environments. The Digital Personal Data Protection Act, 2023 (DPDP Act) includes many provisions to protect individual's data privacy and confers certain functions on the Department of Cyberspace Management. These and similar points should be incorporated into the CCPA Guidelines to counterbalance the deleterious effect of dark patterns, which is an important issue facing Internet privacy regulations and standards. However, the Justice B.N. Report of the Srikrishna Committee suggests that we could consider holding individual groups to a "fiduciary duty" standard. This viewpoint seems plausible based on contemporary legal developments: Many organisations are essentially deceiving and leveraging the trust users place in them. It is important for this to be an effective strategy even when such behaviour falls outside the explicit scope of present regulations. Enough note was made, in other words, at the expense of innocent users. Missing this technical analysis means that even if the CCPA is the ultimate regulator body this is only one possible answer for how digital ecological future problems--including data privacy, consent and algorithmic decisionmaking--will actually play-out in our society. The CCPA Guidelines contain no clear relationship between dark patterns and data privacy violations as well as similar issues. On the other hand, the Data Protection Board (DPB), constituted under Section 19(3) of the DPDP Act, consists of experts in managing data as well as protecting consumer interests and is surely the better body to judge such cases. Hence, an integrated system of regulation, combining the enforcement powers of the CCPA with the technical expertise of the DPB, would be a more thorough and effective way to address this intersection of dark patterns, digital consumer rights, and data privacy in India.。。

Above all: a closer examination is necessary on this issue before effective regulation can be Guidelines Among these will be inconsistencies in the drafting, which can lead to entirely different readings even among consumer courts. Thus the Guidelines specifically state that Annexure I contents are illustrative and that uses/handlings amounting to culpability will be decided according to the specific facts and circumstances. On the other hand, by number 5, it is a putative regulation. Any platform that engages in what appears as such on Annexure I is 'regarded as practising dark pattern'. This apparent contradiction between illustrative and compulsory provisions may confuse regulators as well as businesses. In addition, sometimes the Guidelines' definitions and examples are generic or overlap one another, or are not sufficiently detailed. For instance, SaaS billing is characterised as "using underhand payment methods of credit card searching to trick consumers," yet words like "underhand" are not defined. This terminology thereby risks inadvertent confusion with current credit card fraud, which is the province of the Reserve Bank of India. "Rogue malware" is another dark pattern cited, and yet the definition is not set down more clearly. The Guidelines can be interpreted to point in any given direction as to whether it only deals with guileful software connected to transactions specifically, or more generally targets malicious programming everywhere. Another limitation comes Linux the fixed nature of definitions. With digital technology advancing so quickly, odds are high that new kinds of dark patterns will appear in the future. By listing the specific types of dark patterns, the Guidelines may inadvertently create an unfilled zone in the licensing area of those minor changes within a larger category 'manipulative practices" outside its jurisdiction. A more principle-based approach might have been easier to adapt over time, with greater flexibility. Such a model would have focused on the underlying activity—deception. rather than forcing itself into specific categories. Also, there is a lack of clarity in the Guidelines about how consumers can distinguish between legitimate business practices and the dark pattern. For example, when payment details are requested after taking a free trial, some of the instances included in "sucking mode" are also included.

However, many platforms globally require you to provide credit card information as part of cashiering routine - not because they want to deceive Well, if a use of a design is for commercial purposes, then proving the designer intended to manipulate that design is very difficult indeed. This means it could hinder sanctions being effective if the burden of proof remains on consumers. On top of this, the Guidelines say nothing about remedying infractions, making reparations or taking action against perpetrators. Without a clear statement of how consumers can seek relief and what course that will involve with enforcement authorities, there is little stimulus for users to lodge complaints. For example, while it is certainly irritating to have a platform repeatedly nag a user to download an app, the subsequent damage might not be tangible enough to make legal sense. This absence of meaningful consequences could discourage people from reporting and detract from the practical effectiveness of the Guidelines. The CCPA Guidelines are an important first step in addressing digital manipulation in India, although its present framework is riddled with gaps. The problems with over-elaborate drafting, narrow definitions of the subjects at stake, procedural uncertainties or inconsistencies, and lack of any real sanctions provide ample argument for a more flexible regulatory approach focused on basic principles. Through interpretation by lawyers, and with tests in the courts, the efficacy of these Guidelines will be assured. From this it is evident that India still has significant ground left to cover in its law on dark patterns.

FOREIGN LAW AND ITS IMPLICATIONS ON DARK PATTERNS

1. EUROPE: DIGITAL SERVICES ACT (DSA) AND GDPR

a. DIGITAL SERVICES ACT (DSA):

As a starting point, this regulation is without precedent. It entered into force on 2022 with one basic goal: to make the online environment safe again! In particular, among its several mandates is that it reminds online platforms (especially the very big ones) identify, report and mitigate systemic risks in their services. There are a number of risks. these include dark patterns that manipulate the user interface, disinformation, and content which might actually hurt users' decision-making input. Platforms should take transparency actions, as well themselves be subject to risk assessments and offer an accessible means of reporting for their users. Invalid operations can be meted out hefty fines equivalent to a percentage of an organisation’s global turnover, and regulators are given the power to compel operators into submission. These are robust ways to hold platforms to their commitments.

Unlike the CCPA Guidelines, in which the language and structure of 13 dark patterns are listed with their definitions, the Digital Services Act sets out five general criteria for a framework. India's existing regulations do not require online platforms to perform active risk assessments or lay down preventive measures. Furthermore, statutory penalties for the CCPA Guidelines fail to exist in practice, while the Digital Services Act does stipulate financial sanctions which gives better motivation for non-compliance avoidance.

b. GENERAL DATA PROTECTION REGULATION (GDPR):

GDPR treats the processing of personal data across the EU. It has been effective since 2018. The requirement for consent is a significant feature, which to be valid consent must be given legitimately, freely informed, specific and unambiguous. This is a direct attack on dark patterns that devious slyly exploit cognitive biases to force consent for collection of data, for example through a pre-checked box, misleading prompts or cunning interface design. GDPR gives the authority to originals punish violations of up to 4% annual global turnover as fines. This guarantees that organisations will strive to appeal transparently and humanly to users, rather than to a data collector.

The CCPA `s Guidelines touches on manipulative consent practices, but regulation dark patterns to this implies data protection obligations are not incorporated. GDPR`s enforceable framework ensures a user's right to autonomy over personal data is protected legally, while India's current Guidelines is non-binding and without legal repercussions resulting for actions that use dark patterns to exploit personal data. Limiting their practical enforcement is their real pity.

2. UNITED STATES: BUSINESS AND ROSCA FAIRNESS ACT

a. FEDERAL TRADE COMMISSION (FTC) ACT: The FTC Act, implemented in 1914, is the backbone of U.S. consumer protection law. It prohibits unfair or deceptive acts or practices in commerce (UDAP). In the virtual world, this includes manipulative online designs, false advertising, and dark patterns that may fool people into making unwanted purchases or passing on personal information. The FTC is entitled to investigate violations, bring enforcement actions, and impose financial penalties. What is striking about the Act is an emphasis on preventing and correcting violations. The FTC can require companies to redesign deceptive interfaces or websites, make consumers go back their money, or cease illegal practices of whatever kind. Enforcement thus becomes both preventive and corrective, with strong legal sanctions to protect consumers. Comparison to CCPA Guidelines: The CCPA Guidelines do name 13 specific "dark patterns," but they do not have statutory authority to impose fines or order remediation activities. The CCPA Guidelines primarily serve as advisory guidelines, and unlike the Federal Trade Commission's Act, which gives U.S.regulators clear enforcement powers including fines and corrective orders, this severely limits what level of real-world compliance is realistic.

b. RESTORE ONLINE SHOPPERS' CONFIDENCE ACT (ROSCA):

Shoppers' Confidence Restoration Act (ROSCA) came into force in 2005, targeting negative option marketing. In this kind of marketing, consumers are automatically enrolled in subscriptions unless they actively opt out. ROSCA's core objective is to set standards for subscription traps and safeguard subscription pricing, including clear terms of disclosure, simple cancellation procedures and mandatory permission to ask for regular payments. Enterprises that violate ROSCA will suffer civil penalties or an injunction curtailing their activity, also they must make refund payments. This combination of mechanisms hits the wrongdoer at both ends – reduce opportunity to act badly in future and provide compensation to consumers previously wronged by them. ROSCA also stresses transparency and consumer control. It is unlawful for businesses to employ manipulative methods in order to hide costs or consent procedures. CCPA Guidelines also comprise subscription traps and coercive subscription practices as dark patterns; however, there are no legal penalties in its provisions at present and without voluntary compensation mechanisms either. ROS-CA adopts Western-style legal standards that are clear and can be enforced. Its measures are an effective deterrent to harmful practices, in marked contrast with India's guidelines, presently dependent on consumer complaints or self-regulation without formal statutory backing.

3. UNITED KINGDOM: CONSUMER PROTECTION FROM UNFAIR TRADING REGULATIONS (CPRS)

The UK's primary legal framework on unfair commercial practices, the Consumer Protection from Unfair Trading Regulations 2008 (CPRs), applies both online and offline manipulative and deceptive marketing tactics. CPRs outlaw practices that mislead, coerce or otherwise result in distortion of consumer decision-making. Such examples include false claims, aggressive marketing methods, hidden charges and fraudulent subscription practices.The CPRs adopt a principle-based approach. To judge whether a practice has conformity with its rules the CPRs consider its effect on economic behaviour rather than specifying binding regulations of forbidden practices. This makes it possible as new manipulative forms arise and digital practices emerge for regulators to tailor enforcement activity to suit, ensuring comprehensive consumer protection.

The Competition and Markets Authority (CMA) and other designated regulators carry out enforcement under the CPRs. The CMA may investigate complaints, impose fines, order remedial action, or require businesses to change their misleading practices. This regulation is both preventive and corrective. The judiciary also empowers courts to levy penalties based on harm to consumers in a particular instance, without having to demonstrate that the business had some kind of intent deceive.

Comparison with CCPA Guidelines: On the other hand, the lists compiled by China's CCPA Guidelines contain 13 specific types of dark patterns and provide descriptive examples. Enforcement procedures largely depend on whether or not the malpractice has been intended, requiring proof that the platform deliberately sought to confuse consumers. This approach introduces subjectivity and creates ambiguity in enforcement, particularly for new or only lightly modified types of misleading behaviour. Moreover, the CCPA Guidelines have no statutory basis for imposing penalties or ordering remedial measures, which limits their actual ability to deter harmful conduct. Unlike the CPRs, there is no proactive monitoring mechanism in India like the CMA that checks digital platforms for compliance and then acts if they commit any violations.

INDIAN PERSPECTIVE ON REGULATION OF DARK PATTERNS

In India, the arrival of dark patterns in regulation is a significant and welcome step towards consumer protection and digital governance. For years, manipulative user-interface (UI)—like ads that masquerade as content, pre-ticked consent boxes or misleading prompts—remained unchecked because there was no clear legal basis for challenging it. The Guidelines for Prevention and Regulation of Dark Patterns, 2023 (Guidelines) framed under Section 18 of Consumer Protection Act, 2019 (CPA), by Central Consumer Protection Authority (CCPA), have come in to fill the policy vacuum. The guidelines are the first formal recognition that design -decisions can be a form of unfair trade practice when they end up manipulating, deceiving or coercing users into behaviour they never wanted. This change in strategy is indicative of India's increasing focus on consumer choice and transparency as well as digital ethics in a rapidly economy.

The CCPA's regulations are wide-ranging and potentially have a broad scope. They also apply to all organisations that do business online in a digital arena, such as providers of online platforms, sellers and advertisers. Importantly, the guidelines also apply to overseas companies targeting Indian consumers thus forcing accountability even on foreign lands. This is an extraterritorial extension that recognises the global nature of online business and intends to make sure foreign companies cannot use jurisdictional fractures to leverage deceitful design. The guidelines specifically list some dark patterns – like confirm shaming, nagging, forced engagement, interface interference, reverse information hierarchy tricks and bait-andswitch design – as unfair business practices. So this listed practice has two roles: telling the regulators and platforms what is legal, while not requiring consumers to know how they were actually misled or harmed.

One of the strengths in how India has approached it is by linking it to a data protection and privacy regime. The Digital Personal Data Protection Act (DPDPA) 2023, establishes the free, specific and informed consent in data processing. Dark patterns, of course, violate exactly that consent by influencing user behaviour—forcing them to "agree" or "continue" rather than truly and knowingly consenting. Designs which obscure or guilt individuals into sharing personal information may therefore fall short of the latter requirements consent obligations under the Act. By associating dark patterns with data privacy, India's framework emphasises the need to view deceptive designs as not just unethical but also potentially in contravention of statutory obligations imposed by data protection legislation.

There are also legal consequences to dark patterns well within the realm of cyberlaw, primarily IT Act 2000. This could be used as a basis for "rogue malware," transit data modification, or coercive scripts that deny user free will under tamper/unauthorized access/computer system damage statutes if done without consent. The guidelines provide support to the protective objective of IT Act by CCPA, whereby deceptive online practices such as interface manipulation or hidden tracking can now potentially expose entities to liability under both an unfair trade practice regime and cyber offence. The new Intermediary Guidelines and Digital Media Ethics Code Rules, 2021, found importance here as intermediaries are mandated to exercise due diligence against the hosting or posting of information that is fraudulent, immoral and misleading. Therefore, the platforms should refrain from deploying such interfaces and advertisements filled with dark patterns of coercion, deceit and inescapable engagement that manipulate the users or undermine their trust.

Although it is a step in the right direction, there are several pitfalls with India's regulatory takedown of dark patterns. Industry respondents during stakeholder consultations raised concerns regarding regulatory overlap, definitional confusion and potential burden of compliance. Others said that the guidelines could cast too wide a net, punishing wellintentioned persuasive design or personalisation methods that improve user experience. Others pointed out grey areas in enforcement of the rules — specifically, whether violations of rules against dark patterns automatically get penalised under the CPA or are subject to adjudication separately. Despite these criticisms, CCPA's final guidelines made relatively modest changes. It added new sections such as "SaaS billing traps" and "trick questions"; tied the element of pecuniary gain to motive; and deleted two provisions that would dilute enforcement by limiting the CPA's reach.

In all, India's regulatory model portrays a unified and multi-layered strategy to combat dark patterns through aligning consumer protection, privacy and technology laws. The framework acknowledges that manipulation in the digital environment is not merely a design problem, but also a legal and ethical concern relevant to user rights, user autonomy, and fair market practices. In the future, enforcement will rely on coordination among regulators like the CCPA and organisation such as the Data Protection Board, and capacity-building to conduct audits at scale for detection dark patterns. Public awareness and consumer digital literacy is equally important to enable users of the internet to recognise and oppose manipulative designs. At its core, as an approach to regulation in India, this reflects a maturing understanding of consumer welfare in the digital era—one that acknowledges that considerations around innovation and utility need to be weighed against transparency, fairness and autonomy-building blocks in the online economy.

PSYCHOLOGICAL IMPACT OF DARK PATTERNS

A significant modern aspect of digital design that is both admirable and troubling, dark patterns can thrive on various quirks in human psychology to make the goals set by designers and online entities easier to achieve, often unconsciously fulfilling strategies exactly as their creators wish. At the heart of dark patterns is the belief that users should be manipulated into making choices they would not otherwise consider, to their detriment in the long run. This manipulation can take many forms, from subtle suggestions to straightforward lies, yet all generally functions as a way of bending user wants to fit more closely with designer design.

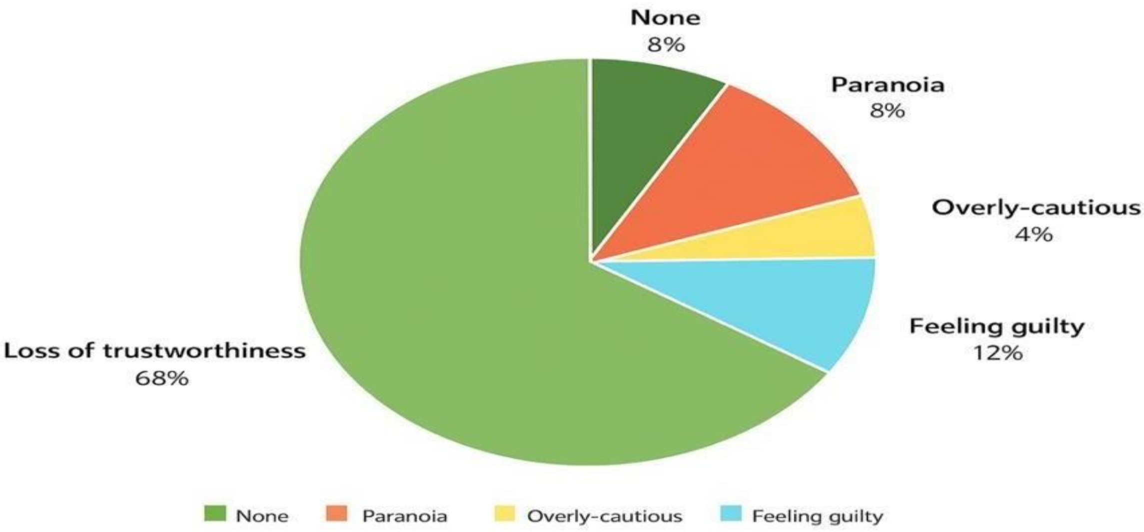
One popular practice among dark pattern designers is to employ the strategic use of colours. Many psychological studies have demonstrated that colour is able to greatly influence how humans view and behave in their environments. The yellowness of autumn apples can make them more attractive- people in dark-defined financial areas often know this far better than those living in rural splendour, we are told. For example, the colour orange is often employed to catch people's attention and create urgency in the viewer, while softer colours such as light grey may give rise to feelings of peace and detachment. If users see a disparity between these visual cues then they are more likely statistically to become aware of and remember the glaring difference, which can create confusion or hesitation in the decision-making process for them. Users interact with online platforms in a way due in part to this psychological manipulation. The next section is a list of research projects and conversations I have had with users.

Both designers and users must understand what psychological manipulators are about, because it demonstrates how misleading elements can enter online pages. Many people fall unwittingly into such traps as these due to their lack of awareness of or innocent attitude towards the real purpose behind these designs. A survey of 25 patients found worrying statistics about the psychological impact these dark patterns have. Three of the patients interviewed (and this is out 25) said that they felt guilty because the manipulative designs which used them to do things made them as people seem like criminals. And besides that, a full 17 patients said that the platforms employing these dark patterns lacked trustworthiness.

Only one person felt totally immune to these emotions, while responses from two more expressed several degrees of negativity. The most commonly reported emotions were trepidation with 11 respondents saying that they felt overly cautious as they browsed the Internet. Two also said that they experienced paranoid thoughts: dark patterns can make people not only trustful of websites but even within their own social circle they aresuspicious.

In the words of Ashley Firth, a leading practitioner and writer in user experience design: Dark patterns do more than just cause discomfort; they can have a significant effect on mental health. Firth notes that these manipulative techniques add to the level of stress which people in general already exist under in their daily lives.

The effects caused by dark patterns are something not to be taken easily. Special or panic disorder sufferers, if they are faced with these tricks in a design just intended to manipulate them, may experience enormous trouble seeking help at all. This will lead to feelings of isolation on your own and being powerless among others there too. Severe exposure to dark patterns has, in some cases, led to panic attacks or even thoughts of suicide. This makes the crying need for widespread recognition and good design practices on networks most pressing indeed. As we negotiate through an ever more complex online world, must notice the psychological effects of dark patterns and fight for open and honest digital relations.



RECOMMENDATIONS

Dark patterns are deceptive design practices implemented on websites and apps intended to coerce users into making decisions that serve businesses at the expense of autonomous choice. Various steps can be taken, at legal, regulatory as well as ethical and educational levels, to address this emerging issue. These guidelines provide a systematic way to address the practice of dark patterning in order for consumers to be safeguarded from psychological abuse.

1. STRENGTHENING LEGAL AND REGULATORY FRAMEWORKS

There should be a robust legal framework which sets out explicitly and prohibits dark patterns. Governments can simply add clauses concerning manipulative online designs to the consumer protection laws which they already have in place. For example, Section 18 of the Consumer Protection Act, 2019 provides powers to the authorities to control unfair trade practices in India and it can be extended even further explicitly as far as technology manipulation is concerned. And the Dark You Can't Breathe in Act for 2023 should be mandatory, not merely recommendatory. This will make online giants accountable for misleading consumer interfaces that trick people into purchases and subscriptions they did not want. It is also essential to have transparent penalties and remedies that apply in case of non-compliance.

2. EFFECTIVE ENFORCEMENT AND MONITORING MECHANISMS

Making laws is one thing; enforcing them is another. Specialised units, or digital investigation cells should be set up within consumer protection regulators to take on cases related to manipulative design. Routine audits and inspections of digital interfaces should be mandatory for large online retailers and digital service providers. Independent ethics boards could also audit the design of websites and mobile apps to ensure they meet fair design standards.

Preemptive regulation of this sort would deter businesses from using dark patterns as a sales tactic.

3. PROMOTING TRANSPARENCY AND DISCLOSURE

It is transparency that forms the foundation of fair consumer choice. Platforms must be mandated to share, in readily understandable language, all critical information about pricing and renewal terms, as well as ease of terminating service or data collection methods. All consent mechanisms should be explicit (e.g., not embedded in a complex menu or prechecked). The opt-out process (or call-to-deactivate the service) should be as easy as the optin (getting-registered). This doctrine, also known as "symmetry of design," is what keeps things fair and helps companies from playing designed frustration games to keep us tied in.

4. ENCOURAGING ETHICAL AND USER-CENTRIC DESIGN

The centrality of online design had to change from optimising profit to the welfare of the user. How interfaces are made must be thoroughly ethical. Designers and developers need to be educated on identifying manipulative features and discouraged from implementing them. [Editor's note: Governments or international organisations could establish a "Fair UX Certification" to acknowledge platforms that adhere to ethical considerations in their digital design.] It would not only generate greater confidence for consumers but airing competition on trust and fairness rather than just on manipulation.

5. CREATING AWARENESS AMONG CONSUMER AND DIGITAL LITERACY

An educated consumer is the best protection against manipulation. Education and awarenessraising efforts should familiarise users with dark patterns and how to make informed digital decisions. Schools, universities, NGOs and government bodies working in tandem can inculcate digital literacy at a young age. Consumers should also be educated on their legal entitlements and the measures of grievance redressal at hand. Public resources, like a national database of known dark patterns, can also assist users in remaining informed and vigilant.

6. GLOBAL COOPERATION AND POLICY HARMONISATION

Online markets go beyond borders, so international cooperation is needed. Countries could draw inspiration from global best practice, notably EU's Digital Services Act (DSA) and the

United States Federal Trade Commission (FTC) guidelines for addressing misleading digital practices. International standards can also be used to make sure that multinationals adhere to the same ethical rules everywhere in the world. India and other developing countries must take part in global deliberations to harmonise their policies in this regard.

7. ENSURING PSYCHOLOGICAL AND ALGORITHMIC SAFEGUARDS

A lot of dark patterns play on human psychology and cognitive biases. Hence, rules should also cover the design of algorithms and recommendation systems. People should be entitled to turn off personalised nudges or targeted ads that leverage their emotions, fears and time urgency. Renewing consent periodically should be required in order for users to maintain control of data and the implications associated with their choices. The protections would also guard against over-dependence on automated systems that take advantage of human psychological vulnerabilities.

CONCLUSION

Dark patterns have become one of the more worrisome problems associated with today's digital economy, as more and more bicarbonate is mixed up in a grey slurry between persuasion and manipulation. Such tricks of design or deception use human psychology and bias in behaviour to steer consumers into decisions which favour businesses, usually without their willing knowledge. With the increasing importance of digital transactions in every aspect of our daily lives, there is a real danger that these deceptive interfaces become not only an effort to undermine consumer rights but more fundamentally the principle of trust within digital markets. This problem is best addressed by a multi-faceted effort. Legal and regulatory frameworks must be developed or enhanced to articulate, outlaw, and sanction the use of dark patterns. It should give enforcement agencies the power and technical ability to watch over digital platforms and make sure these rules are followed. As important are the promotion of ethically designed, user-centred principles that value transparency and informed consent (Nissenbaum 2009, Nissenbaum & Introna 2010) as well as fairness in online exchanges (Dourish & Bell 2007). Education and understanding are also important to create resilience in the consumer. Through improved digital literacy, people are better able to spot manipulative approaches and consequently take informed decisions. In addition, by collaborating internationally and implementing global best practices, how to regulate can become less fragmented and more efficient as some models can be replicated in different jurisdictions –

look at the EU Digital Services Act or guidelines from U.S. Federal Trade Commission rules for instance. At the end of the day, preventing dark patterns is not a regulatory issue alone, but indeed an ethical obligation to protect consumer autonomy and dignity in today's digital era. An open and honest digital ecosystem will be the key for bringing consumer trust back and that technology is serving mankind instead of manipulating it."

BIBLIOGRAPHY

1. Dark patterns guidelines https://www.nls.ac.in/wpcontent/uploads/2021/04/Dark-Patterns.pdf
2. Dark pattern regulation in US and UK - https://www.finnegan.com/en/insights/articles/dark-patterns-regulation-in-the-uk-andus.html
3. Europe dark pattern guidelines and law - https://epthinktank.eu/2025/01/14/regulating-dark-patterns-in-the-eu-towards-digitalfairness/
4. Reshaping india dark pattern guidelines towards a better digital landscape https://www.lawrbit.com/article/reshaping-indias-dark-pattern-guidelines-towards-abetter-digital-landscape/
5. https://repository.nls.ac.in/ijclp Part of the Consumer Protection Law Commons, and the Contracts Commons
6. Deep dive into dark pattern regulation in India - https://ijcrt.org/papers/IJCRT2402257.pdf