# THE ALGORITHMIC MIRAGE: RE-EVALUATING 'INFORMED CONSENT' IN THE AGE OF GENERATIVE AI AND PREDICTIVE PERSONALIZATION

Adutiya Jha, Symbiosis Law School, Nagpur

**ABSTRACT**

As Generative AI evolves from an analytical tool to the primary architect of the consumer experience, the way we perceive the concept of consumer protection is being radically transform. Established benchmark like "The Average Consumer", "Consent" are no longer relevant with the development of "Dark Patterns 2.0," the concept of a digital marketplace as one "Market of Many" has shifted to one "Market of One", since Generative Artificial Intelligence creates temporary hyper personalized choice architectures based on what it learns about the cognitive and emotional responses of each avenue user on a continual basis.

This article identifies a systematic failure in the notices and consent regime created by India's Consumer Protection Act (CPA) 2019 and the 2023 Guidelines on the Prevention and Regulation of Dark Patterns. This static frameworks cannot match the "velocity of harm" in an AI-Driven environment. Through a comparative analysis, the research explores the eroding line between digital persuasion and illegal algorithmic manipulation.

A large part of this research focuses on what has been termed the "Black Box" issue, which addresses the inability for consumers to prove that they have been manipulated, as the evidence (a consumer AI-generated interface's result) is lost the moment a transaction is completed. To bridge this, the paper provides a "Techno-Legal" framework involving mandatory "Algorithmic Audits" for large e-commerce companies and require companies to provide real time labelling on AI-generated marketing. Crucially, it advocates shifting the burden of proof to corporations when systemic deception is identified.

This research supports moving from a narrow view of "Consumer Welfare" to a broader definition of "Digital Dignity." This will be accomplished by integrating Online Dispute Resolution (ODR) and creating strong standards for Algorithmic Transparency this research offers a pathway to protect Consumer Sovereignty in an age where the Algorithm knows you better than you know yourself.

**Keywords:** Generative AI, Consumer Protection Act 2019, Dark Patterns, Algorithmic Manipulation, Informed Consent, Digital Dignity.

## I. INTRODUCTION

### BACKGROUND OF THE PROBLEM

Historically, consumer protection laws were originally set up for a traditional environment of transactions (i.e., a physical store or a website). The rise of Generative AI has introduced an entirely new concept of hyper-personalization through automated technologies, meaning that today's sales rely less on the standard approach to advertising and instead focus more on "manipulating" the consumers based on their individual psychological states at the time of the interaction with a product or service. This new method of reaching consumers will completely change the way the laws that govern the relationship between consumers and businesses are interpreted and applied (i.e., the legal doctrine of "Caveat Emptor" and the standard of the "Average Consumer").

### PROBLEM STATEMENT: THE EROSION OF PERSONAL LIBERTY

The erosion of personal liberty is evident in the problem statement. The core of the problem is the fact that Generative AI uses the "Information Asymmetry" that consumer law tries to bridge, as evidence by the Consumer Protection Act (CPA), 2019 and the Dark Pattern Guidelines of 2023 in India. These laws were intended to protect consumers from fixed deceptive designs, such as pre-checked boxes. However, they are currently not designed to address the new type of deceptive design called "Dynamic Deception."

Three dimensions are affected by this problem:

i) AI exploits consumer vulnerabilities by determining when they are most impulsive (for instance, late at night or after completing a sequence of clicks) and creates a fake offer called a "Limited Time Offer."

ii) Because the users have to close the tab containing the AI-generated interface, there is no evidence of the unfair practice of deceptive design as the evidence is transient.

iii) If the consumer is persuaded (or "nudged") to make a purchase because an algorithm knows the psychological triggers of that consumer better than they do, the final action of that consumer (the click) may not have been made freely. Instead, the consumer's action may have been coerced by the algorithm.

## RESEARCH QUESTION

1. In what ways will the introduction of Generative AI into the UI/UX Design Process fundamentally change the legal definition between allowed “persuasion” & illegal “manipulation of consumers”?

2. How do the unfair trade practices provisions under CPA 2019, along with the CCPA Dark Pattern Guidelines, give adequate protection to consumers against AI-generated deceptive design?

3. In what ways can the inclusion of 'Techno-Legal' governmental frameworks as they relate to these areas of preventative policy protection from 'Dark Patterns 2.0' be used to strengthen the Indian Consumer Protection Act, 2019, and the CCPA Dark Pattern Guidelines? For example, does the inclusion of EU AI Act 'Unfairness' rulings, US Federal Trade Commission, China’s provisions on Algorithmic Recommendation Systems, Israel’s Innovation for All policy, Russia’s fifth package of Digital Antimonopoly legislation, South Korea’s Artificial Intelligence Basic Act, or UAE’s ethical standards on Artificial Intelligence create support for the Indian Consumer Protection Act, 2019, and the CCPA Dark Pattern Guidelines in preventing Dark Patterns 2.0?

4. How do we suggest creating a “Road Map” for establishing due process standards for determining liability due to the use of algorithm-created models as Black Boxes?

5. Will implementing “Algorithmic Audits” and reversing the burden of proof reinstate the principle of “Informed Consent” in eCommerce?

## OBJECTIVES

1. To examine the components of “Dark Patterns 2.0” via Generative AI's technological capabilities.

2. To assess the extent to which the Consumer Protection Act 2019 meets the needs of predictive analytics.

3. To develop a “Techno-Legal” scale that transitions from a focus on “Notice” to a focus

on “Algorithmic Transparency”

## METHODOLOGY

The methodology chosen for this research is a Comparative Doctrinal Methodology. It compares Indian consumer law with developing international AI regulations (i.e. the European Union's AI Act and United States Federal Trade Commission Staff Report) in order to highlight areas where divergences exist. The reason for this significant analysis is because as India is currently positioning itself as a global leader in Artificial Intelligence field, this paper can act as an important resource for the policy makers to make sure that technological advancements align with maintaining the integrity of “Digital Dignity” and the rights of consumers.

## II. THE RISE OF “DARK PATTERNS” 2.0: FROM STATIC NUDGES TO ALGORITHMIC COERCION.

The digital marketplace is undergoing a radical transition in the way consumers make decisions. Nearly a decade ago, “Dark Patterns” (meaning UI design choices that make it easier for consumers to accidentally make a purchase, be led astray, or otherwise misled) were largely static. The advent of Generative Artificial Intelligence (GenAI) in UI/UX (user experience and user interface) design has led to the emergence of “Dark Patterns 2.0,” which are much more sophisticated fast moving, dynamic, personalised, and ever evolving.

### How “Hyper-Personalized” Deception Works?

Traditional marketing uses broad demographic categories to target its audience whereas GenAI creates “persuasion profiles” that are uniquely created each time someone interacts with a product. GenAI performs “cognitive hacking” by leveraging people's cognitive biases (e.g., Loss Aversion, Sunk Cost Fallacy) when a person is most likely to succumb to the perpetrator's manipulation.

### The Legal Divide on Using Persuasion to Manipulate (the difference)

The primary legal dilemma is understanding the line between using persuasion (commercial speech that is protected) and manipulating (the invasion of the consumer's ability to choose). In India, there is a set of tests within the country’s court cases that gives us some initial ideas as to where that line may be drawn:

### 1. The Commercial Speech Right to Know v. Commercial Speech

The fine work of Tata Press Limited v. Mahanagar Telephone Nigam Limited (1995)[1] developed the idea that "commercial speech" is a protected form of speech under Article 19(1)(a) of the Constitution of India[2], as it is part of the public's "Right to Know".GenAI-driven Dark Patterns (like Interface Interference and Confirm Shaming) are a violation of that "Right to Know." With the use of AI to generate an interface that either hides material information or attempts to shame users for not selecting a subscription plan, the generated interface has lost its protected status as "commercial speech," and becomes an act that the user may take action against in the courts.

### 2. An Average Consumer v. Marginal Vulnerability

Historically, Indian Courts have relied on the Average Consumer standard in determining whether a reasonable person sees an advertisement and believes it to be true or not. This was essentially the premise that the "average consumer" test were based upon. For example, in case of Colgate Palmolive (India) Ltd. v. Hindustan Unilever Ltd.[3] the Hon'ble Court articulated a standard between where puffery would be considered permissible; yet misrepresentation will remain. Now, since AI is able to develop an adaptive response or even an adaptive attack vector based on information provided (user profile, age, shopping behaviours); it has rendered the average consumer standard to no longer apply here. AI provides an adaptive response to the user while creating a legal burden now being transferred to the algorithm's intent and actions.

### 3. Unfair Contracts and Lack of Alternatives

Under the Consumer Protection Act (CPA), 2019, Section 2(46), defines the term 'unfair contract'[4] as one which 'substantially modifies the rights of a consumer' when entering into it. In the case of Pioneer Urban Land & Infrastructure Ltd. v. Govindan Raghavan (2019)[5], the Hon'ble Supreme Court stated that unilaterally imposed ' take it or leave it' contracts are voidable in nature if there is no option for the consumer under

[1] *Tata Press Ltd v Mahanagar Telephone Nigam Ltd* (1995) 5 SCC 139
[2] Constitution of India 1950, art 19 (1)(a)
[3] *Colgate Palmolive (India) Ltd v Hindustan Unilever Ltd* 1999 SCC OnLine SC 774
[4] Consumer Protection Act 2019, s 2(46)
[5] *Pioneer Urban Land & Infrastructure Ltd v Govindan Raghav* 20

those conditions. When a Gen AI environment creates a situation called a 'Retention Loop' (the user getting lost in complex AI-created pathways when trying to terminate service) this generates technological duress against consumers. Thus, according to the ratio of Pioneer Urban, consent obtained through such an environment is not free, is obtained through coercion and is an example of an Unfair Trade Practice.

**4. Algorithmic bias and default settings**

The effectiveness of "default bias" in the regulation of digital interfaces has recently come under review in light of recent developments within the regulatory environment of India. In the case of Google LLC. v. Competition Commission of India (2023)[6], the Competition Commission of India (CCI) upheld by the National Company Law Appellate Tribunal (NCLAT) found that Google was guilty of using "default settings" to limit consumer alternatives to choosing Google products. This is an important precedent for establishing the principle of "Choice Architecture". For a GenAI-based marketplace to use the practice of automatically selecting items (e.g., adding them automatically to the shopping cart of a customer) or to apply an "algorithmic self-preferencing" component, it would violate the principle of consumer autonomy that is laid down by Google.

**The Concept of a Dark Pattern Loop an Impact on Consumer Autonomy**

As previously stated in the CCPA's guidelines released in 2023, 13 different types of "Dark Patterns" have been identified, one of which includes "False Urgency," as well as "Subscription Traps."[7] In the most recent CCPA advisory of June 2025, the fact remains that digital platforms will continue to utilize more sophisticated and often AI-driven variations of existing patterns to exploit Consumer Autonomy. The legal analysis must be focused on how the platform generates its interface versus what it looks like. If the process for creating a product's design relied primarily on an algorithm to optimize for "behavioural modification" (which is a way of operating without rational thought) instead of "Delivering Information," then this would be an example of prohibited consumer manipulation, as referenced in Section 2(47) of the Consumer

[6] *Google LLC v Competition Commission of India* 2023 SCC OnLine SC 88

[7] Ministry of Consumer Affairs, Food & Public Distribution, E-Commerce Platform Urged to Self-Audit and Eliminate Dark Patterns: Centre' (Press Information Bureau, July 22, 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2146813.

Protection Act of 2019.[8] In short, the integration of GenAI into the design process transition the traditional forms of "passive" deception into a form of "active" coercion. Based on the rulings of Tata Press (Right to Know) and Pioneer Urban Land (Meaningful Choice), it should be noted that AI-generated Dark Patterns constitute not simply unethical design practices but, systemic breaches of Indian Consumer law.

**Evaluation of the Current Mechanisms: The CPA 2019 and CCPA Guidelines**

The fundamental question to consider is whether the Indian Legislation is adequately equipped to protect consumers from complex, AI-driven deceptive advertising in 2026. The CPA 2019 and CCPA prevention and control guidelines for Dark Patterns address the challenge, but the application of Dark Patterns 2.0 impacts their effectiveness due to a static-centric basis.

1. **Broad Definition of "Unfair Trade Practices" (UTP)**

   Under Section 2(47) of CPA 2019, Unfair Trade Practices (UTPs) are defined broadly and extensively to include any 'unfair method or deceptive practice'. The Judiciary has consistently expanded this section by applying a broad has consistently expanded this section by applying a broad interpretation toward UTP's past. The Hon'ble Supreme Court stated in Godfrey Phillips India Ltd. v. Ajay Kumar (2008)[9] that the key factor for determining a UTP is to be guided by the 'tendency to mislead or deceive', regardless of actual damages occurring at the beginning.

   The ability of UTPs to provide "adequate protection" is being undermined by the "Subliminal Nature of AI Manipulation". Historically, UTP violations have been limited to deception acts of an overt nature such as giving false statements about the weight, quality, or price of a product. Deceptive designs created with AI usually present truthful information in a coercive manner. For example, an AI may indicate to a user who is identified "highly anxious" that "10 People Are Looking at This Hotel" by displaying that information in pulsating red lettering, while the user may have already been exposed to the identical message displayed in a normal font in the same advertisement. The deception is not in the information itself, but in how it is presented in a coercive manner based on the user's level of anxiety. Lawsuits under current UTP

[8] Consumer Protection Act 2019, s 2(47)
[9] *Godfrey Philips India Ltd v Ajay Kumar* 2008 SCC OnLine SC 603

case law are unable to address "Truthful Coercion," where damage is psychological as opposed to a factual.

## 2. The CCPA Guide: A Reactive Approach to Fighting the Battle

The CCPA Dark Pattern Guide, 2023 is a significant step in defining what constitutes dark patterns and outlines certain types of conducts, including 13 specific practices known as "Nagging," "Subscription Traps" (Sausalito), "Bait and Switch" and more. While this information is helpful, this still does not provide an adequate guide to navigating these practices. It only provide an adequate guide to navigating these practices. It only provide an adequate guide to navigating these practices. It only provides example of dark patterns, rather than outlining how to avoid them.

There are two separate issues that exist with the taxonomy provided in the guide:

i. Taxonomy Trap: By clearly stating what patterns are considered dark patterns, it creates an opportunity for "Regulatory Arbitrage," as generative AI can create its own design to manipulate consumers using "Grey Patterns." Just because it doesn't meet the exact criteria of 13 Patterns identified, it does not mean it cannot be used to manipulate individuals. For instance, instead of creating a "False Urgency" to manipulate the consumer to make a purchase, an AI could utilize "Emotional Optimization" by soothing the consumer's emotions to lower their defenses and present a high-cost add on product after they have been lulled into a "safe" space emotionally.

ii. The CCPA guidelines are outcome-focused: They impose sanctions based on how users interact with the final product (the interface). However, in this age of GenAI, these interfaces change regularly. The CCPA must therefore adopt a process-focused approach to ensure it adequately captures bad actions taken by algorithms. Thus, the CCPA must regulate algorithms based on what their goal is; for instance if you trained an algorithm to maximize short-term conversion while minimizing consumer benefit, you created the violation at the time you trained the algorithm, long before the consumer ever saw the instant interface.

### 3. Proof Value and Evidence Collection

The CPA 2019 poses several significant challenges to the concept that adequate protection must be provided under an enforceable contract; chief among these challenges is the evidentiary burden of proof that a consumer was mislead falls upon the consumer, as indicated in SGS (India) Ltd. v. Dolphin International Ltd.,(2021)[10], which affirmative stated that the burden of proving a fraudulent or deceptive was on the individual making the complaint. With the advent of generative artificial intelligence (GenAI), it is nearly impossible for a consumer to ISDA provision against the "Black Box" effect of this technology. Genetic material generated by an AI can be more closely tailored to an individual consumer, and the material will not exist long enough for the purchaser to collect comparative evidence demonstrating that the consumer was treated differently than others. It is likely, therefore, that there will be a time lag that the consumer or user is able to take a "snapshot" of the interface generated by the AI. Additionally, the CCPA does not currently provide for reversing the burden of proof in situations where the consumer may have been misled by an algorithmic product, resulting in a situation where the consumer has a right to make an allegation against an algorithmic provider, but that right does not possess the ability to obtain any type of compensation or remedy.

### 4. The Fallacy of "Notice and Consent":

At present, much of Indian law is based on "Disclosure." The California Consumer Privacy Act (CCPPA) guidelines suggest that by providing clear labels, many Dark Patterns may be avoided. But, as shown by behavioral economics research (used to develop the EU AI Act) and its understanding of how designs are algorithmically optimised to exploit the "System 1" (unconscious) brain response, the "System 2" (rational) method of disclosure or "Fine Print" is invalid when a user has been manipulated using Hyper-Personalisation.

According to Central Inland Water Transport Corporation Limited v. Brojo Nath Ganguly (2007)[11], awareness above the law/market place should give "weaker party" protection from being exposed to "unconscionable" contractual terms. Therefore, if an

[10] *SGS (India) Ltd v Dolphin International Ltd* AIR 2021 SC 4849
[11] *Central Inland Water Transport Corpn Ltd v Brojo Nath Ganguly* 2007 SCC OnLine Mad 734

AI creates Hyper-Personalisation to take advantage of a user's rational ability to make "Informed Consent", then the "Disclosure" against the user's wishes is inconsequential because the user's ability to create "Informed Consent" has been algorithmically stolen.

Although the Consumer Protection Act (CPA) 2019 and the 2023 Guidelines create a skeleton framework for Consumer Protection, these frameworks do not possess sufficient strength in terms of a "Techno-Legal" framework to stop Generative AI. The present framework is akin to bringing a knife to a gunfight; it is sufficient to protect the "Static Deceptive" market of 2010s, but is not sufficient for the "Dynamic" manipulation that will occur in 2026. In order to ensure adequate protection, the law must not only ban the design of the regulation but also regulate the algorithmic intention that creates the designs.

## COMPARATIVE LEGAL ANALYSIS: THE INDIAN FRAMEWORK AND THE "AI GAP"

The transition from "Dark Patterns 1.0" (Static deceptive design) to "Dark Patterns 2.0" (dynamic, AI-driven manipulation) requires a shift from traditional consumer protective laws to new "Techno-Legal" regulatory frameworks. The Indian Consumer Protection Act 2019 and the CCPA Guidelines establishes basic "conduct-based" rules yet they do not include the comprehensive "architectural oversight" available in new international legal systems. The regulatory approaches used by EU countries USA, China, Israel, Russia, South Korea and UAE create a pathway which helps India expand its legal framework through new statutory measures.

### Architectural Accountability: Lessons from the EU, China, and the UAE

The European Union's AI Act has created a new regulatory framework called a "Techno-Legal" approach by focusing on they way an AI system interfaces with consumers (through its UI) and applying it to how the AI system creates the interface (through its algorithm). As written in Article 5 of the EU AI Act, AI systems that utilise "subliminal techniques" or exploits age or economic vulnerabilities to deceive consumers to use their products are specifically prohibited under EU law[12]. This change provides a definitive framework for the Indian Consumer

[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelling Act) [2024] OJ L1689, art 5(1)(b)

Protection Act on what constitutes a specific harm represented through the UI and how should these be compensated, rather than waiting for a consumer being defrauded before defining what constitutes a certain harm or unfairness caused by an AI system. Likewise, China has created an algorithmic filing approach to pre-register mechanical recommendation services in their 2022 Algorithmic Recommendation Provisions. These provisions allow for prior disclosure of each mechanical recommendation system to a regulatory agency so that the same agencies are able to monitor how all mechanical recommendation service mechanism operate and possibly prevent "information cocoons" and "price discrimination"[13] situations that the Indian Consumer Protection Act currently does not and cannot handle effectively under section 2(47) until the harm has already occurred. The 2024 UAE AI Ethics Charter further creates a basis for more substantial and profound processes when designing or developing AI systems through the emphasis placed on "Human Oversight." The Charter provides the foundation for more expansive legislation and historic precedent for ensuring the overall consumer and public interest remains protected though both the Command and Control Model and the Self Directed Model of Development. An allowance for an "Algorithmic Kill-Switch" and neutrality in the interface options available to consumers, as opposed to simply relying on a simplistic notice and consent approach, create the framework for additional regulatory and legal avenues for consumers to pursue for damages and harm caused through the refinement of the UI and mechanisms recommendations.[14]

Bridging the Black Box via South Korea, Israel, and the United States of America:

South Korea and the U.S., as well as Israel, work together to make AI technologies easier for consumers to understand and use by bridging the gap between consumer-producer relationships and the "Black box" nature of AI technology. The "Evidentiary Gap" represents a challenge to the District Commissions under Indian Laws because it prevents consumers from being able to prove how an AI influenced their decisions. In an effort to overcome this difficulty, South Korea's AI Basic Act (2025) establishes two main methods that assist consumers in identifying how they were influenced by the AI "Explanation" and "Domestic Representation."[15] South

[13] Provisions on the Administration of Algorithmic Recommendation for Internet Information Services 2022, art.17.
[14] Office of the Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications, 'The UAE Charter for the Development and Use of Artificial Intelligence' (4 July 2024) https://uaelegislation.gov.ae/en/policy/download/the-uae-charter-for-the-development-and-use-of-artificial-intelligence accessed 1 February2026.
[15] Act on Promotion of Artificial Intelligence Industry and Framework for Establishing Trustworthy Artificial Intelligence 2025 (South Korea) art 12

Korea requires that consumers be able to access an explanation of how high-impact AI systems influenced their decisions and permits the placement of a "Domestic Representative" on behalf of a non-domestic platform in order to ensure that a local court can question the use of an algorithmically influenced "Black Box" by the platform[16]. In addition, the "Responsible Innovation" policy (2023) established by Israel has taken this idea one step further by utilizing the existing sectoral regulators to enforce "Bot Disclosure," which requires consumers to know when an AI engages their emotional brains (System 1) rather than human engagement[17]. The Federal Trade Commission of the United States (FTC's) Project Artificial Intelligence Compliance (2024) and the agency's use of Section 5 of The Federal Trade Commission Act to target "Means and Instruments of Deception" provides a model for holding developers of artificial intelligence (AI Developers) liable for the "deceptively potential" characteristic of their technological creations (i.e., tools used by AI Developers), rather than solely to the entity that operates the platform[18]. The unique combination of the three concepts (Accountability in a Local Context, Transparency, and developer accountability) provides India with a strong "Techno-Legal" framework to revise its definition of "Unfair Contracts" under Section 2(46) of the Indian Contract Act.

**Tackling Algorithmic Coercion: Learning from the USA and Russia**

The combination of Competition and Consumer Laws will be necessary to combat the economic coercion of Digital Patterns 2.0, which utilizes pricing methods (Dynamic Pricing) as well as new fees (Junk Fees). As outlined in Russia's 5th Antimonopoly Package (2023) with the introduction of the new Network Effect, Russia has added this new data point to assist authorities in identifying companies operating an algorithm that is being manipulated by the platform to restrict consumer choice. By recognizing an algorithm as a "Carriers-Generator of Agreements," Russian State Law allows for the examination of what appears to be dynamic pricing patterns, however, under examination, these types of pricing patterns are shown to be

[16] Cho Jung-woo 'Could You Be Fined for AI Content? What to know About Korea's Latest Technology Law' Korea JoongAng Daily' (Jan. 25, 2026) https://koreajoongangdaily.joins.com/news/2026-01-25/national/socialAffairs/Could-you-be-fined-for-AI-content-What-to-know-about-Koreas-latest-technology-law/2507223. accessed 14 January 2026.

[17] Ministry of Innovation, Sci. & Tech., 'Responsible Innovation: Israel's Policy on Artificial Intelligence Regulation and Ethics' (December 2023) https://www.gov.il/BlobFolder/policy/ai_2023/en/Israels%20AI%20Policy%202023.pdf. Accessed 17 January 2026

[18] Federal Trade Commission, 'FTC Announces Crackdown on Deceptive AI Claims and Schemes' ( Press Release, Sept. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes. accessed 21 January 2026

predatorily manipulative.[19] This concept will provide the theoretical foundation for the Indian CCPA to equally investigate Algorithmic Self-Preferencing and Price Gouging as unfair Trade Practices (Section 2(47)) and competition violations not just by looking at them through the lens of Competition Law. Likewise, the US FTC's ruling regarding Deceptive Fees (Click-to-Cancel rule) will allow the FTC to use specific Process-Based transformations to bring an end to the practice of creating Roach Motels and Subscription Traps and provide consumers with a clear path toward understanding and selecting their product offerings. It is evident that for India's Digital Market to adequately protect the concept of Digital Dignity, a legal requirement must accompany Consumer Education to enforce that every consumer has a right to the formulation of a legislature that legitimately guarantees the principle of Interface Neutrality and makes sure that the design of the Digital Market's Choice Architecture in 2026 will parallel the design of the Physical Market that was created based upon the Indian CPA of 1986. The original CPA of 1986 assured consumers transparency within the physical marketplace, via weight, measures, and labels, while the modern legislature needs to ensure that the digital "nudge" does not turn into a digital "shove". By establishing Process-Based Standards, India will create an environment in which the Informed Consent principle is not a legal fiction found within the code of a black-box algorithm.

## THE "BLACK BOX" DILEMMA REGARDING DISPUTE RESOLUTION: A BLUEPRINT FOR ALGORITHMIC DUE PROCESS.

Consumer protection and rights are governed by the Consumer Protection Act (CPA), 2019. The CPA is designed to empower consumers against the overwhelming control of producers over them. With the introduction of Generative AI, however, the relationship between the producer and consumer has flipped upside down, creating a situation where traditional methods of proving product liability may no longer be viable. In a typical case of defective products, consumers could take advantage of physical evidence, such as a bottle of adulterated soda or defective brake pads, and use res ipsa loquitur as the basis for establishing producer liability. However, many Dark Patterns 2.0 are created through "Black Box" algorithms that generate personalized, ephemeral interfaces that leave no physical evidence of their creation and often disappear after the transaction has been completed. This has created a significant "Probative Gap," where the consumer is required to demonstrate that the Black Box code was the source

[19] Federal Law No. 301-FZ of July 10 2023 on Amendments to the Federal Law "On Protection of Competition" (Fifth Antimonopoly Package) [2023] Sobranie Zakonodatel'stva Rossiiskoi Federatsii No. 29, Item 5335

of the manipulation although they are unable to see, understand, or access the Black Box code. In order to provide the consumer with a means to overcome this significant gap, a procedural "Road Map" is needed to outline clear standards for due process that will ensure that the opacity of AI does not provide producers with a shield of impunity.

The legislative shift in burden of proof outlined in the First Step of the Road Map is necessitated by the recent ruling in Citicorp Finance (India) Ltd. v. Snehasis Nanda (2025)[20]. In this case, the Hon'ble Supreme Court of India reaffirmed its strict interpretation of the burden of proof, concluding that a consumer could not establish his or her case solely by identifying the weakness or silence of the other party. Even where a company has failed to file a specific denial to a complaint, the burden of establishing the underlying factual basis remains with the consumer. Although the above process would work for traditional contracts in a physical format, this approach will create an unfair system where a consumer is not able to subject an opaque AI system to scrutiny because that consumer lacks the necessary skills to locate, inspect and interpret the basic programming that applies to that manipulation. Therefore, a possible method to overcome this situation is to have the Indian Government's legal system adopt a rebuttable presumption of causation within the Consumer Protection (General) Rules. Under this proposed new standard, when a consumer presents a prima facie case demonstrating they have been exposed to a Dark Pattern such as a subscription trap or a confirmshaming interface, then immediately, the platform will have the burden to disprove that the platform is not responsible for misleading that consumer. This approach is consistent with the EU AI Act's "High Risk" classification that states that if a corporation uses a "black box" to interact with customers, that corporation will ultimately be required to demonstrate that their algorithm acted in a manner that was not misleading. After the burden of proof shifts, the second stage of the "roadmap"-"Mandatory Algorithmic Audits"-must be put into effect to obviate a platform's claim that they are unaware of the decision-making processes of their system. The "Black Box" defense, in which a company asserts that they cannot explain the rationale behind the AI's "hallucinated" fraudulent offer, needs to be procedurally eliminated. Following from the frameworks of China's Algorithmic Filing Regime and the UK's ICO Framework regarding the requirement of transparency, the largest e-commerce business need to be required, through the inclusion in pre-trail discovery, to maintain and produce a "Black Box Log". This "audit" functions as a digital analogue to the "black box" flight recorders and provides insight into the

[20] *Citicorp Finance (India) Ltd v Snehasis Nanda* 2025 SCC OnLine SC 594

environmental optimization preference of the AI (e.g., “Maximize User Welfare”; “Maximize Time on App”) and documents the decision pathways taken by the AI to reach the ultimate recommendations presented to the litigant. Therefore, the inability to produce this landmark result in an “Adverse Inference” against the platform and shall be treated as an admission of the allegation made against them, thus transforming the “Black Box” from an asset in a defence case into a liability.

Lastly, the hearing or trial of evidence will need to evolve too, to accommodate the technical evidence. A District Consumer Commission (DCC) will not be able to understand and interpret complex neural network weights or Python code without assistance. As a result, an outline for the marketplace must include the appointment of "Digital Amicus Curiae", provided for in Section 38(9) of the CPA 2019[21]. Digital Amicus Curiae assist DCCs in obtaining expert opinions. Digital Amicus Curiae will aid in translating the Digital Audit results into legal definitions of "Unfair Trade Practices," similar to the evolution of strict liability under the South Korean AI Basic Law; the DCC does not have to find a malicious intent (Mens Rea) in the code, the mere existence of deception in the final design of an algorithm regardless of the developer's intent is enough to impose liability. Further, the suggested model will evolve the framework of Consumer Protection Law from its historical passive Caveat Emptor (Let The Buyer Beware) model to a more proactive Inquisitorial model that provides the “Right to Information” contained in the CPA 2019[22] including a substantive right to understand how and why he is being targeted by an algorithm.

## RECOMMENDATIONS ON A NEW FRAMEWORK FOR INDEPENDENCE IN DIGITAL TRANSACTIONS

The “Consent Crisis” in the Age of Algorithms the main goal of this research is to answer the question, “Will allowing for the use of Algorithm Audits and shifting the burden of proof to verify ‘Informed Consent’ in eCommerce?” This research is dependent on the unfortunate fact that, in today’s digital ecosystem, ‘Informed Consent' is merely a legal fiction. Traditional structures for “Notice and Consent,” which originally required the consumer to read and voluntarily provide written acknowledgment of their acceptance of the terms being proposed to them, have now become ineffective due to “Dark Patterns 2.0.” For example, many users

[21] The Consumer Protection Act 2019, s 38(9)
[22] The Consumer Protection Act 2019, s 2(9)(ii)

now click the "I Accept" buttons on sites where the users has not read or understood what it is they are consenting to, and which have been deliberately designed to take advantage of various cognitive biases with a hyper-personalized, time-accelerating elements that cause users to feel as if they have no choice but to accept the terms presented in front of them.

The reason that consent is breaking down is both a lack of consumer vigilance and structural differences in power between platforms, who have "God-like" access to data, and cnsumers, who are operating in an information void. Therefore, increasing transparency by showing users what every agreement they are making looks like is not sufficient. To get back to the substance of what was meant to be consent (the "meeting of minds" or consensus ad idem) as required by the Indian Contract Act of 1872 the law needs to step into changing how the architecture of the digital marketplace was created This paper proposes three areas for reform :

1. Mandating disclosure via AI labelling
2. Legislatively reversing the burden of proof
3. Integrating mandatory Online Dispute Resolution (ODR).

**Mandating Disclosure via AI Labelling**

The first area of focus in the new framework relates to the customer's right to know as it relates to the Consumer Protection Act of 2019 which is outlined in Section 2(9)(ii). Currently, many customers do not know that they are dealing with an AI as their 'agent' or that what they are being charged is based on an individualised algorithm rather than a fixed market price. If the customer does not know this information, then any consent that they have provided is voidable if it is based on misleading information. We recommend that there be an amendment to the Consumer Protection (E-Commerce) Rules 2020 to require a "Digital Watermark" or an "AI Icon", similar to how a product has to be marked with either a "Veg" or "Non-Veg" symbol, on any interface element which has been made relevant to a consumer by way of an algorithm. The purpose of this level of transparency is the same as the disclosure obligations contained within Article 50 of the EU AI Act[23]. A consumer should not only be notified that they have been shown something according to an algorithm, but the reasons for that decision should also

[23] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act ) [2024] O.J. (L) 1689, art 50

be disclosed; therefore, the consumer would see exactly what the "Primary Optimization Goal" of the algorithm was that resulted in their interface element being presented to them. This legal basis for this requirement is firmly established in the seminal decision of the Supreme Court of India in Central Inland Water Transport Corporation v. Brojo Nath Ganguly (1986)[24] where the Court stressed that any "unconscionable" contract term (such as where there is gross inequality of bargaining power) is an invalid term and as such will be struck down by the Courts. By treating the failure to disclose the purpose of the algorithm as a means of achieving constructive fraud and/or "active concealment" and by applying the requirements of the "meeting of the minds" (i.e., meeting the consumer's needs), the law can ensure that the "meeting of the minds" (consensus ad idem) is not merely a theoretical construct created by the ingenuity of clever programmers, but rather is a true display of the consumers' freedom to choose. The decision regarding Pioneer Urban Land & Infrastructure Ltd., Govindan Raghavan, SC (2019), supported the finding that one-sided provisions of an agreement created by asymmetrical information are "unjust", so therefore not enforceable. This means that the requirement of Disclosure will allow "the black box" to no longer act as a mechanism for psychological coercion but turn it into a mechanism whereby consumers will have the opportunity to make a reasonable, informed, voluntary and legally enforceable decision related to the transaction.

**Legislatively Reversing the Burden of Proof**

The Second area to address the work of transforming the "Duty of Algorithmic Care" to a new procedural framework that transfers it from being a "vulnerable consumer-centric" requirement to one that is placed upon the more technically competent online platform. Today, the existing adversarial model, as confirmed by the Supreme Court in Citicorp Finance (India) Ltd. v. Snehasis Nanda, created a nearly insurmountable challenge for the plaintiff to establish what terms they entered into and whether or not they acted with deceptive intent (i.e., the terms of the "transaction") as a result of the defendant's manipulation of technology (i.e., the terms of the "transaction"). This is particularly unreasonable when using "Black Box" systems, as the evidence of causation for the transaction would exist in proprietary format and ultimately hidden within the encrypted transaction logs. Therefore, to address this gap, we are proposing an introduction of "Causation Rebuttable Presumption" to be implemented under the Consumer Protection (General) Rules, aligned with the logic embodied in Section 106 of the Indian

[24] *Central Inland Water Transport Corpn v Brojo Nath Ganguly* (1986) 3 Supreme Court Cases 156

Evidence Act of 1872 (Section 109 of the BSA of 2023)[25], which provides that the burden of providing proof rests with the person that has the "special knowledge" of the circumstances relevant to their claim. If a consumer can prove that they were exposed to a widely recognized Dark Pattern, such as a Subscription Trap or a False Urgency prompt, then the burden of proof will shift to the platform for the algorithm to establish it acted with neutrality and fairness. To prove otherwise, the platform will need to produce an independent Algorithmic Audit and failure to do so will result in an Adverse Inference. This new approach to liability moves the focus from Intent to Outcome, consistent with other emerging strict liability laws for AI failures. By making it mandatory for platforms to monitor deceptive outcomes of their self-learning algorithms, the law reinstates accountability on the part of corporations because they cannot use a technical glitch as a defence from the programmed manipulation legal consequences of their actions.

**Integrating mandatory Online Dispute Resolution (ODR).**

The final area to address the urgent necessity of having an enforcement mechanism that is digital-native through making Online Dispute Resolution (ODR) mandatory for all small-value e-commerce disputes. The existing Consumer Commissions in India are unable, both functionally and physically, to accommodate the enormous number of low-value disputes that occur in the digital economy, where it is not appropriate for the ₹500 "junk fee" dispute to be litigated over the course of many years. Therefore, we propose that ODR be made mandatory for disputes that come under some pecuniary threshold, and that an API connecting these platforms to the ODR institutions, which are empaneled by the government, be integrated. The ODR institutions will have a three-tiered approach to resolving the dispute, whereby the process begins with an automated negotiation process, and progresses through to human mediation and finally to binding arbitration within a maximum of 45 days after the initiation of the ODR process. This is consistent with the NITI Aayog's ODR Policy (2021)[26] and will ensure that "digital justice" will keep pace with the growth of digital commerce. What safeguards the integrity of such a process is an ODR platform’s use of blockchain-based “evidence lockers” to create an immutable record of cryptographically hashed screenshots of the user interface at the exact moment the transaction occurs. A tech-legal solution to

[25] The Indian Evidence Act 1872, s 106 ; Bharatiya Sakshya Adhiniyam 2023, s 109
[26] NITI Aayog, ‘The Future of Dispute Resolution: The ODR Policy Plan for India’ (October 2021) https://www.niti.gov.in/sites/default/files/2023-03/Designing-The-Future-of-Dispute-Resolution-The-ODR-Policy-Plan-for-India.pdf. accessed 14 February 2026

preventing “evidence spoliation” whereby, once a complaint is made, the platform has modified its user interface to erase any evidence of a Dark Pattern which is the use of these blockchain records as the primary evidentiary source under the IT Act 2000. Thus, the “Digital Amicus Curiae,” who is an expert in data science and empaneled under Section 38(9) of the CPA 2019, will have a factual record from which to make an objective determination. By digitizing the adjudicative process and creating a secure chain of evidence, this framework allows for both consumer rights to be protected at law and enforced in real-time.

## CONCLUSION:

India's digital marketplace faces an unprecedented challenge in today’s time. At this paper shows, the rapid of “Dark Patterns 2.0” spurred by Generative AI and “Black Box” algorithms has changed the legal meaning of the seller-buyer relationship. The traditional doctrine of Caveat Emptor (the buyer is responsible for his/her own purchase) assumes that there will be a level financial playing field and that the buyer can protect themselves from fraud as long as they are aware of the risk; however, in this new reality, the seller holds more power than the buyer, and because of this new asymmetry between buyers and sellers, “Informed Consent” has become meaningless, and the buyer is forced to mindlessly click an agreement through heavily coerced means instead of making an informed agreement based on their understanding of how the seller's business operates. This research indicates that although the lifetime of the Consumer Protection Act (2019) and the Digital Personal Data Protection Act (2023) provides a valid sword and shield against sophisticated predatory harm, they alone do not provide sufficient evidence or cause under either statute. Although these laws provide substantive rights to obtain information and thus provide some protection against unfair trade practices, both statutes do not contain the procedural tools needed to penetrate the corporate "Veil" of algorithmic construction. As previously articulated in this paper, bridging this "Probative Gap" will involve much more than simply enforcing some three-year statute of limitation or some similar civil action against a corporation for a violation of the statute(s); i.e. it will also require a proactive restructuring of the digital "Choice Architecture". A roadmap for the transformation described here is provided with the guidance of a three-section plan: Mandatory Labelling of AI; The Reversal of the Burden of Proof; and The Inclusion of Mandatory On-Line Dispute Resolution (ODR). The above-mentioned mandatory labelling of AI will give back to users their cognitive independence by allowing them to know the intentions behind the algorithms used by the platform. By reversing the burden of proof through the application of the

evidentiary principles found in Section 106 of the Indian Evidence Act, 1872 which is now in Section 109 of the Bharatiya Sakshya Adhiniyam (Evidence Act), 2023-the "Black Box" will no longer serve as a safe haven for those wishing to exploit others. In addition, the conversion of the dispute resolution process into a digital format will make remedy as accessible as the transaction itself. The reforms aim to create human-centered innovations which drive their implementation forward. The digital economy must evolve from a system of "Algorithmic Coercion" to one of "Digital Dignity," where the interface serves the user rather than subverting them. Indian consumers will become nothing more than data points for extraction if the law fails to keep pace with technological advancements. If India adopts these recommendations, the country will establish a new global standard of jurisprudence which replaces the outdated warning of Buyer Beware with the essential requirement of Caveat Algorithm (Let the Algorithm Beware). The implementation of our system guarantees that Artificial Intelligence will protect human rights through its ability to maintain independent decision-making power.