

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

---

Volume 9 | Issue 2

---

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

---

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact [support@vidhiaagaz.com](mailto:support@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# Manufactured Consent Dark Patterns and the Legal Limits of Consumer Autonomy in Digital Markets

---

RAKSHIT SHARMA<sup>1</sup> AND ADITI SHARMA<sup>2</sup>

## ABSTRACT

*The rapid expansion of digital markets has transformed how consumers interact with businesses, but it has also enabled the widespread use of dark patterns, interface designs that subtly manipulate user behaviour. This paper examines the concept of “manufactured consent,” where consumer choices are shaped not by informed decision-making but by psychological nudges embedded within digital platforms. By integrating legal analysis with insights from behavioural psychology and management strategy, the study explores how businesses leverage cognitive biases such as default effects, loss aversion, and decision fatigue to influence user actions, often at the cost of genuine autonomy.*

*From a legal perspective, the paper evaluates the adequacy of existing regulatory frameworks, including data protection and consumer protection laws, in addressing these manipulative practices. It highlights the challenges regulators face in distinguishing persuasive design from exploitative manipulation, particularly in jurisdictions like India where enforcement mechanisms are still evolving. From a managerial standpoint, the study analyses how dark patterns are deployed as strategic tools to maximize engagement, conversion rates, and data extraction, raising questions about ethical governance and corporate responsibility.*

*The paper argues that traditional notions of consent are increasingly inadequate in the face of psychologically engineered interfaces. It calls for a reconceptualization of consent that accounts for behavioural realities, alongside stronger regulatory interventions and ethical design standards. Ultimately, the study contributes to the growing discourse on the intersection of law, psychology, and management by demonstrating how digital architectures are reshaping the boundaries of consumer autonomy and legal accountability.*

**Keywords:** *Dark Patterns; Manufactured Consent; Consumer Autonomy; Digital Market Regulation*

---

<sup>1</sup> Author is a Student at Amity University, Noida, Uttar Pradesh, India.

<sup>2</sup> Author is Assistant Professor at Amity University, Jharkhand, India.

## I. INTRODUCTION

The rapid expansion of digital markets has fundamentally altered the relationship between consumers and businesses, shifting traditional transactions into complex, data-driven interactions. Online platforms today are not merely intermediaries of exchange but sophisticated environments engineered to influence user behaviour. Through the integration of algorithmic design and behavioural insights, corporations increasingly shape how choices are presented, perceived, and ultimately made. This transformation raises a critical legal and managerial question: whether consumer consent in digital environments remains genuinely informed and voluntary, or whether it has become a constructed outcome of psychological manipulation.

One of the most contentious manifestations of this shift is the rise of “*dark patterns*,” a term used to describe user interface designs that subtly steer individuals toward decisions that benefit the platform, often at the expense of the user’s interests.<sup>3</sup> These practices include pre-selected options, misleading prompts, hidden costs, and complicated opt-out mechanisms that exploit cognitive biases such as default preference, loss aversion, and decision fatigue.<sup>4</sup> While such techniques may increase user engagement and profitability, they simultaneously blur the line between legitimate persuasion and unlawful manipulation.

From a legal standpoint, the doctrine of consent has long been central to consumer protection and contractual legitimacy. However, in digital contexts, consent is frequently reduced to a single click on lengthy and complex terms that users rarely read or fully understand.<sup>5</sup> This formalistic approach raises doubts about whether existing legal frameworks adequately capture the realities of behavioural influence embedded in modern digital design. In India, instruments such as the *Consumer Protection Act, 2019*, and the *Digital Personal Data Protection Act, 2023*, attempt to address unfair trade practices and data misuse, yet their capacity to regulate nuanced psychological manipulation remains uncertain.<sup>6</sup> Comparative jurisdictions, particularly the European Union under the General Data Protection Regulation, have begun recognizing the limitations of traditional consent models, but enforcement challenges persist.<sup>7</sup>

From a managerial perspective, the deployment of dark patterns is not accidental but often

---

<sup>3</sup> Harry Brignull, *Dark Patterns: Inside the Interfaces Designed to Trick You*, DARKPATTERNS.ORG, <https://www.darkpatterns.org> (last visited Apr. 30, 2026).

<sup>4</sup> Cass R. Sunstein, *The Ethics of Influence: Government in the Age of Behavioral Science* 21–45 (2016).

<sup>5</sup> Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* 3–12 (2014).

<sup>6</sup> The Consumer Protection Act, No. 35 of 2019, INDIA CODE (2019); The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

<sup>7</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1.

reflects deliberate strategic choices aimed at maximizing conversion rates, data extraction, and user retention. In highly competitive digital markets, firms face strong incentives to optimize behavioural outcomes, even when such practices raise ethical concerns. This creates a tension between corporate profitability and consumer autonomy, where legal compliance may not necessarily align with ethical responsibility.

This paper seeks to examine the phenomenon of “*manufactured consent*” through an interdisciplinary lens, integrating legal analysis with insights from behavioural psychology and management theory. It argues that the current legal conception of consent is increasingly inadequate in addressing the realities of digitally mediated decision-making. By analysing regulatory frameworks, psychological mechanisms, and corporate strategies, the study aims to demonstrate how dark patterns undermine genuine consumer autonomy and challenge the effectiveness of existing legal protections. Ultimately, it calls for a reconceptualization of consent that reflects behavioural realities and for the development of more robust regulatory and managerial responses to safeguard consumer interests in the evolving digital economy.

## II. CONCEPTUAL FRAMEWORK: PSYCHOLOGY OF MANIPULATION

Understanding dark patterns requires a shift from purely legal analysis to the underlying psychological mechanisms that shape human decision-making in digital environments. Contemporary behavioural research demonstrates that individuals do not make decisions as fully rational actors; instead, they rely on cognitive shortcuts, or heuristics, which are systematically predictable and exploitable.<sup>8</sup> Digital platforms leverage these cognitive tendencies to subtly guide users toward outcomes that align with corporate objectives, often without the user’s conscious awareness.

One of the most significant psychological mechanisms exploited in digital design is the default effect, wherein individuals tend to accept pre-selected options rather than actively changing them.<sup>9</sup> In online environments, this manifests through pre-ticked consent boxes, automatic subscriptions, or default privacy settings that favour extensive data sharing. Closely related is loss aversion, a principle suggesting that individuals perceive losses more intensely than equivalent gains.<sup>10</sup> Platforms exploit this by framing choices in a way that emphasizes potential losses, such as missing out on benefits or features, if users opt out, thereby nudging them toward compliance.

---

<sup>8</sup> Sendhil Mullainathan & Eldar Shafir, *Scarcity: The True Cost of Not Having Enough* 12–25 (2021 ed.).

<sup>9</sup> Alessandro Acquisti, Laura Brandimarte & George Loewenstein, Privacy and Human Behavior in the Age of Information, 347 *SCI*. 509, 509–14 (2020).

<sup>10</sup> Daniel Kahneman, *Thinking, Fast and Slow* 282–90 (updated ed. 2021).

Another critical factor is decision fatigue, which occurs when individuals are overwhelmed by repeated choices, leading to reduced cognitive capacity and reliance on simplified decision-making strategies.<sup>11</sup> Digital interfaces often present lengthy privacy policies, multiple consent requests, and complex settings menus, effectively exhausting users and encouraging them to select the quickest path, typically “*accept all.*” This creates an illusion of consent, where agreement is given not through informed deliberation but through cognitive overload.

The concept of nudging, derived from behavioural economics, further complicates the distinction between legitimate influence and manipulation. Nudges are subtle design interventions intended to steer behaviour without restricting choice.<sup>12</sup> While nudging can be used for socially beneficial purposes, such as encouraging healthier habits or safer online practices, its application in commercial contexts often prioritizes profit over user welfare. The ethical concern arises when nudges become covert and exploitative, transforming into manipulative practices that undermine user autonomy.

Additionally, framing effects play a crucial role in shaping user decisions. The way information is presented, whether emphasizing benefits or risks can significantly influence outcomes.<sup>13</sup> For instance, presenting a data-sharing option as enhancing user experience, rather than as a potential privacy risk, can lead to higher acceptance rates. Similarly, the use of urgency cues, such as limited-time offers or countdown timers, exploits psychological pressure, pushing users toward impulsive decisions rather than reflective ones.

Importantly, these psychological mechanisms operate within broader social and organizational contexts. Users often trust established platforms and assume a baseline level of fairness, which reduces their critical scrutiny of interface design.<sup>14</sup> This phenomenon, sometimes referred to as “*automation bias*” or “*platform trust*,” further amplifies the effectiveness of manipulative strategies. From a managerial perspective, these insights are deliberately incorporated into user experience (UX) design to optimize engagement metrics, conversion rates, and data acquisition. The distinction between persuasion and manipulation ultimately hinges on the presence of transparency and user awareness. Persuasion respects user autonomy by providing clear, balanced information, whereas manipulation exploits cognitive vulnerabilities to produce

---

<sup>11</sup> Roy F. Baumeister & John Tierney, *The Power of Bad: How the Negativity Effect Rules Us and How We Can Rule It* 67–75 (2021).

<sup>12</sup> Cass R. Sunstein, *Sludge Audits*, 12 BEHAV. PUB. POL’Y 1, 3–8 (2022).

<sup>13</sup> Timo Dietrich et al., *Nudging and Choice Architecture in Digital Environments: A Systematic Review*, 40 J. BUS. RES. 1, 5–10 (2022).

<sup>14</sup> Nir Eyal, *Hooked: How to Build Habit-Forming Products* 45–60 (rev. ed. 2021).

outcomes that users might not otherwise choose.<sup>15</sup> In digital markets, this boundary is increasingly blurred, as sophisticated design practices operate beneath the threshold of conscious recognition.

Thus, the psychology of manipulation reveals a fundamental tension between human cognitive limitations and technologically enhanced persuasion strategies. Legal frameworks that rely on formal notions of consent fail to account for these behavioural realities. Without integrating insights from psychology, regulation risks addressing only the surface of the problem while leaving the underlying mechanisms of influence intact.

### III. DARK PATTERNS AS CORPORATE STRATEGY

Dark patterns are not accidental design flaws or isolated ethical lapses; they are increasingly embedded within corporate strategy as deliberate tools to influence user behaviour and optimize business outcomes. In highly competitive digital markets, firms rely on data-driven insights and behavioural analytics to refine user experience (UX) design in ways that maximize engagement, conversion rates, and long-term retention.<sup>16</sup> What appears to the user as a neutral interface is, in reality, a carefully engineered system aimed at guiding decision-making in directions that align with corporate interests.

At the core of this strategy lies the monetization of attention and data. Digital platforms operate within an economic model where user interaction translates into revenue, whether through targeted advertising, subscription models, or data extraction.<sup>17</sup> Dark patterns serve as a mechanism to reduce friction in user decision-making processes, ensuring that users take actions beneficial to the platform, such as consenting to data collection, completing purchases, or remaining engaged for longer durations. For instance, “roach motel” designs make it easy for users to sign up for services but deliberately complicate the process of cancellation, thereby increasing customer retention and recurring revenue.<sup>18</sup>

Similarly, forced continuity strategies, where free trials automatically convert into paid subscriptions without explicit reminders, exploit user inattention and inertia.<sup>19</sup> Hidden costs, another common form of dark pattern, introduce additional charges at later stages of a transaction, capitalizing on the user’s prior investment of time and effort. These practices are not merely technical choices but reflect managerial decisions aimed at optimizing key

---

<sup>15</sup> OECD, *Dark Commercial Patterns* 15–22 (2022), <https://www.oecd.org>.

<sup>16</sup> Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* 88–102 (2021).

<sup>17</sup> Shoshana Zuboff, *The Age of Surveillance Capitalism* 93–120 (updated ed. 2021).

<sup>18</sup> Organisation for Economic Co-operation and Development (OECD), *Dark Commercial Patterns* 27–32 (2022), <https://www.oecd.org>.

<sup>19</sup> Fed. Trade Comm’n, *Bringing Dark Patterns to Light* 15–18 (2022), <https://www.ftc.gov>.

performance indicators (KPIs) such as conversion rates, average revenue per user (ARPU), and customer lifetime value (CLV).

From a management perspective, the integration of behavioural design into corporate strategy is often justified as a response to market pressures. Firms operate in environments where even marginal improvements in user engagement can yield significant financial gains.<sup>20</sup> Consequently, companies invest heavily in A/B testing, behavioural experiments, and data analytics to identify the most effective ways to influence user actions. This creates a feedback loop in which successful manipulative designs are reinforced and scaled across platforms.

However, the strategic use of dark patterns raises serious ethical and legal concerns. While such practices may enhance short-term profitability, they risk eroding consumer trust and exposing firms to regulatory scrutiny.<sup>21</sup> Increasingly, regulators and policymakers are recognizing dark patterns as unfair trade practices, particularly when they distort consumer choice or obscure material information. Yet, from a corporate standpoint, the line between persuasive design and unlawful manipulation remains ambiguous, allowing firms to operate within grey areas of the law.

Importantly, dark patterns also reflect broader issues of corporate governance and accountability. Decisions to implement manipulative designs are often made at the intersection of product development, marketing, and legal compliance teams, highlighting the need for integrated oversight mechanisms.<sup>22</sup> Ethical considerations are frequently subordinated to business objectives, especially in organizations where performance metrics prioritize growth and profitability over user welfare.

Thus, dark patterns function as a strategic instrument within modern digital business models, bridging behavioural psychology and managerial decision-making. They illustrate how corporate strategy increasingly leverages human cognitive vulnerabilities to achieve economic goals. This raises a fundamental question for legal and regulatory frameworks: whether existing approaches to consumer protection can effectively address practices that are not overtly deceptive but are nonetheless systematically manipulative.

#### **IV. LEGAL FRAMEWORK AND REGULATORY RESPONSES**

The rise of dark patterns has compelled regulators across jurisdictions to reconsider traditional

---

<sup>20</sup> Sinan Aral, *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health—and How We Must Adapt* 145–160 (2021).

<sup>21</sup> Harry Brignull, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* 55–70 (2023).

<sup>22</sup> Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 132–145 (2021).

approaches to consumer protection, data privacy, and digital governance. At the heart of the issue lies the inadequacy of existing legal frameworks, which were largely designed for offline transactions and assume rational, informed decision-making by consumers. In digital environments, where behavioural manipulation is embedded within interface design, these assumptions no longer hold true. As a result, legal systems are increasingly attempting to adapt, though with varying degrees of success.

In India, the primary legal response to manipulative digital practices can be traced to the *Consumer Protection Act, 2019*, which prohibits unfair trade practices, including misleading representations and deceptive conduct.<sup>23</sup> While the Act does not explicitly define dark patterns, its broad provisions allow regulators to interpret certain manipulative designs as unfair or deceptive. This gap has been partially addressed through the *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, issued by the Central Consumer Protection Authority. These guidelines identify specific categories of dark patterns, such as false urgency, subscription traps, and interface interference, and seek to prohibit their use in digital platforms.<sup>24</sup> Although these guidelines represent a significant step forward, their effectiveness depends on enforcement capacity and the willingness of regulators to address evolving design practices.

Complementing consumer protection law is the *Digital Personal Data Protection Act, 2023*, which governs the collection and processing of personal data.<sup>25</sup> The Act emphasizes the requirement of “free, specific, informed, and unambiguous” consent, aligning with global data protection standards. However, the practical application of these requirements remains challenging in the presence of dark patterns that subtly coerce users into consenting. The law does not yet fully account for behavioural manipulation that undermines the voluntariness of consent, thereby exposing a critical regulatory gap.

From a comparative perspective, the European Union has taken a more structured approach through the *General Data Protection Regulation (GDPR)*.<sup>26</sup> The GDPR explicitly mandates that consent must be freely given and prohibits practices that impair user autonomy, such as pre-ticked boxes or bundled consent. Furthermore, the *Digital Services Act (DSA)* strengthens these protections by directly addressing manipulative interface designs and requiring greater transparency in platform operations.<sup>27</sup> European regulators have increasingly scrutinized

---

<sup>23</sup> The Consumer Protection Act, No. 35 of 2019, INDIA CODE (2019).

<sup>24</sup> Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023* (India).

<sup>25</sup> The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

<sup>26</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1.

<sup>27</sup> Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act), 2022 O.J. (L

companies for deploying dark patterns, particularly in cookie consent mechanisms and subscription models. Nevertheless, enforcement challenges persist due to the complexity of proving psychological manipulation and the cross-border nature of digital platforms.

In the United States, regulatory responses have been more fragmented, relying primarily on the enforcement powers of the *Federal Trade Commission* (FTC). The FTC has taken action against deceptive design practices under its mandate to prevent unfair or deceptive acts in commerce. Its 2022 report, *Bringing Dark Patterns to Light*, highlights the widespread use of manipulative interfaces and signals a growing regulatory focus on the issue.<sup>28</sup> However, the absence of a comprehensive federal data protection law limits the scope of intervention, leaving significant gaps in consumer protection.

Despite these developments, several challenges continue to undermine the effectiveness of legal responses. First, the distinction between permissible persuasion and unlawful manipulation remains inherently ambiguous. Legal standards often require proof of deception or harm, which can be difficult to establish when manipulation operates subtly through design rather than explicit misrepresentation.<sup>29</sup> Second, enforcement mechanisms struggle to keep pace with rapidly evolving technologies, particularly as companies continuously refine their strategies through real-time data analytics and experimentation. Third, jurisdictional limitations complicate regulation, as digital platforms operate across borders, often exploiting differences in legal standards to avoid liability.

Moreover, existing frameworks tend to focus on outcomes rather than processes, addressing instances of harm after they occur rather than regulating the design practices that produce them. This reactive approach is ill-suited to the dynamic nature of digital markets, where manipulative strategies can be deployed and scaled rapidly. Increasingly, scholars and policymakers advocate for a shift toward *ex ante regulation*, which emphasizes preventive measures such as design standards, transparency requirements, and accountability mechanisms within corporate governance structures.<sup>30</sup>

In sum, while legal frameworks in India and abroad have begun to recognize the risks posed by dark patterns, they remain constrained by conceptual and practical limitations. The persistence of formalistic notions of consent, combined with enforcement challenges and regulatory fragmentation, allows manipulative practices to continue operating within legal grey areas.

---

277) 1.

<sup>28</sup> Fed. Trade Comm'n, *Bringing Dark Patterns to Light* (2022), <https://www.ftc.gov>.

<sup>29</sup> Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 178–190 (2021).

<sup>30</sup> Organisation for Economic Co-operation and Development (OECD), *Dark Commercial Patterns* 45–52 (2022), <https://www.oecd.org>.

Addressing these issues requires not only stronger laws but also a deeper integration of behavioural insights into legal standards, ensuring that regulation reflects the realities of decision-making in digital environments.

## V. GAPS AND CHALLENGES IN EXISTING LEGAL FRAMEWORKS

Despite growing regulatory attention, existing legal frameworks remain ill-equipped to effectively address the nuanced and evolving nature of dark patterns in digital markets. One of the most fundamental gaps lies in the continued reliance on a formalistic notion of consent, which assumes that users make rational and informed decisions when interacting with digital interfaces. In practice, however, consent is often obtained through complex, manipulative designs that exploit cognitive biases, rendering it neither fully informed nor genuinely voluntary.<sup>31</sup> Legal standards that prioritize the presence of consent over the quality of decision-making fail to capture this behavioural reality.

A related challenge is the ambiguity in distinguishing permissible persuasion from unlawful manipulation. Digital platforms routinely argue that interface design choices fall within legitimate business practices aimed at enhancing user experience.<sup>32</sup> However, when such designs exploit psychological vulnerabilities such as default bias, urgency cues, or decision fatigue, the line between influence and coercion becomes blurred. Existing laws, including consumer protection and data protection statutes, often lack precise definitions or thresholds to identify when persuasion crosses into manipulation, creating significant interpretive uncertainty.

Another major limitation is the difficulty of proving harm and intent. Traditional legal frameworks are structured around demonstrable harm or deception, requiring clear evidence that a user was misled or suffered a tangible loss.<sup>33</sup> Dark patterns, however, operate subtly, influencing decisions without overt misrepresentation. The harm is often diffuse and cumulative, such as the gradual erosion of privacy or the normalization of exploitative practices, making it difficult to establish causation or quantify damages in legal proceedings.

Enforcement challenges further compound these issues. Regulatory bodies frequently lack the technical expertise and resources necessary to identify and assess sophisticated interface designs.<sup>34</sup> Digital platforms continuously evolve their strategies through A/B testing and real-

---

<sup>31</sup> Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* 25–40 (2021 ed.).

<sup>32</sup> Harry Brignull, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* 102–118 (2023).

<sup>33</sup> Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 178–190 (2021).

<sup>34</sup> Organisation for Economic Co-operation and Development (OECD), *Dark Commercial Patterns* 33–40 (2022), <https://www.oecd.org>.

time data analytics, allowing them to adapt quickly to regulatory scrutiny. This creates a persistent enforcement gap, where regulators struggle to keep pace with the speed and scale of technological innovation.

Jurisdictional fragmentation presents an additional obstacle. Digital platforms operate across multiple jurisdictions, often exploiting differences in legal standards and enforcement mechanisms to minimize liability.<sup>35</sup> While regions such as the European Union have adopted relatively stringent regulations, others, including the United States, rely on more fragmented approaches. In India, although recent guidelines on dark patterns represent progress, the absence of harmonized global standards limits their overall effectiveness.

Moreover, existing frameworks tend to adopt a reactive approach, addressing violations only after harm has occurred. This ex-post model is particularly inadequate in the context of digital markets, where manipulative practices can be deployed and scaled rapidly, affecting millions of users before regulatory intervention occurs.<sup>36</sup> Preventive mechanisms, such as mandatory design standards or algorithmic audits, remain underdeveloped or inconsistently applied.

Another critical gap lies in the lack of integration between law and behavioural science. Legal doctrines continue to be grounded in assumptions of rational choice, overlooking decades of research demonstrating systematic cognitive biases in human decision-making.<sup>37</sup> Without incorporating behavioural insights, regulation risks addressing only the surface manifestations of manipulation while leaving its underlying mechanisms intact.

Finally, corporate governance structures often fail to adequately internalize legal and ethical considerations related to dark patterns. Decisions regarding interface design are typically driven by business metrics such as engagement and revenue, with limited oversight from legal or compliance teams.<sup>38</sup> This organizational disconnect allows manipulative practices to persist even in environments where formal compliance mechanisms exist.

In sum, the persistence of dark patterns highlights significant structural and conceptual shortcomings within existing legal frameworks. Addressing these gaps requires a shift from formalistic and reactive approaches toward more nuanced, proactive, and interdisciplinary regulatory strategies that account for the behavioural realities of digital decision-making.

---

<sup>35</sup> Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* 210–230 (2023).

<sup>36</sup> Fed. Trade Comm'n, *Bringing Dark Patterns to Light* 25–30 (2022), <https://www.ftc.gov>.

<sup>37</sup> Cass R. Sunstein, *Sludge Audits*, 12 BEHAV. PUB. POL'Y 1, 10–15 (2022).

<sup>38</sup> Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* 140–155 (2021).

## VI. CASE STUDIES

The abstract concerns surrounding dark patterns become clearer when examined through real-world examples, where interface design directly shapes user behaviour and raises questions of legal accountability and consumer autonomy. The following case studies illustrate how psychological manipulation operates in practice and how regulators have responded.

One of the most widely scrutinized examples involves *cookie consent banners* used across digital platforms. Many websites present users with prominently displayed “*Accept All*” options, while the “*Reject*” or “*Manage Preferences*” options are either hidden, less visible, or require multiple steps. This design exploits the default effect and decision fatigue, nudging users toward broad consent for data collection. In *Bundeskartellamt v. Meta Platforms, Inc.*, European regulators examined how such practices contributed to excessive data aggregation without meaningful user consent.<sup>39</sup> The case highlighted that formal compliance with consent requirements does not necessarily ensure substantive autonomy when interface design is inherently manipulative.

A second example can be seen in subscription traps and forced continuity models, particularly in the context of digital services. Companies often offer free trials that automatically convert into paid subscriptions unless users actively cancel within a specified period. The cancellation process is frequently designed to be complex or time-consuming, reflecting a “*roach motel*” pattern. In 2023, the Federal Trade Commission initiated enforcement actions against several companies for deceptive subscription practices, emphasizing that such designs can constitute unfair trade practices.<sup>40</sup> These cases demonstrate how user inertia and inattention are systematically exploited for financial gain.

A third illustrative case involves hidden costs in e-commerce transactions, where additional fees are introduced at later stages of the purchasing process. Platforms may initially display a lower price, only to add service charges, taxes, or mandatory add-ons at checkout. This practice leverages the sunk cost fallacy, as users who have already invested time in the transaction are less likely to abandon it. Regulatory bodies, including the Central Consumer Protection Authority, have identified such practices as misleading and potentially violative of consumer protection laws.<sup>41</sup> Despite this recognition, enforcement remains inconsistent, particularly in rapidly evolving online marketplaces.

---

<sup>39</sup> Case C-252/21, *Meta Platforms Inc. v. Bundeskartellamt*, 2023 E.C.R. (Court of Justice of the European Union).

<sup>40</sup> Fed. Trade Comm’n, *Bringing Dark Patterns to Light* 15–18 (2022), <https://www.ftc.gov>.

<sup>41</sup> Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns*, 2023 (India).

Another significant example arises from app permission requests, where mobile applications seek access to extensive user data under the guise of functionality. Permissions are often bundled together, making it difficult for users to selectively grant access. The design of these prompts frequently emphasizes convenience while downplaying privacy risks, thereby influencing user decisions through framing effects. In *Norwegian Consumer Council v. Google LLC*, regulators argued that such practices undermine informed consent by obscuring the true extent of data collection.<sup>42</sup> This case underscores the tension between technological design and legal standards of transparency.

Finally, interface interference in social media platforms provides a compelling example of behavioural manipulation. Features such as infinite scrolling, autoplay, and intermittent reward systems are designed to maximize user engagement by exploiting psychological triggers related to habit formation and reward anticipation. While these practices may not always constitute direct legal violations, they raise broader concerns regarding user autonomy and mental well-being. Scholars argue that such designs blur the boundary between voluntary engagement and engineered dependence, challenging traditional regulatory approaches that focus narrowly on deception or misrepresentation.<sup>43</sup>

Collectively, these case studies reveal that dark patterns operate across diverse digital contexts, from data consent and subscriptions to pricing and engagement strategies. They demonstrate that manipulation is often embedded within the structure of digital interfaces rather than explicit misstatements, making it difficult for existing legal frameworks to effectively address the issue. These examples reinforce the need for a more nuanced regulatory approach that accounts for both the psychological mechanisms and strategic motivations underlying digital design practices.

## VII. RETHINKING CONSENT: A BEHAVIOURAL-LEGAL APPROACH

The concept of consent occupies a central position in both contract and data protection law, traditionally understood as a manifestation of individual autonomy and informed choice. However, in digitally mediated environments, this classical understanding is increasingly inadequate. The proliferation of dark patterns reveals that consent is often not the product of deliberate and rational decision-making but rather the outcome of carefully engineered

---

<sup>42</sup> Norwegian Consumer Council, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights* 18–25 (2020).

<sup>43</sup> Sinan Aral, *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health—and How We Must Adapt* 145–160 (2021).

behavioural influences.<sup>44</sup> This necessitates a fundamental rethinking of consent through a behavioural-legal lens that accounts for the realities of human cognition and digital design.

At its core, the problem lies in the disconnect between formal consent and substantive autonomy. Legal frameworks typically validate consent if it meets procedural requirements, such as being freely given, specific, and informed.<sup>45</sup> Yet, these criteria assume that individuals are capable of processing information and making decisions without undue influence. Behavioural research, however, demonstrates that individuals are systematically affected by cognitive biases, framing effects, and environmental cues, which can significantly distort their choices.<sup>46</sup> In digital contexts, these biases are not incidental but are actively exploited through interface design, rendering formal consent a legal fiction in many cases.

A behavioural-legal approach seeks to bridge this gap by incorporating insights from psychology into the interpretation and regulation of consent. One key implication is the need to move beyond disclosure-based models, which rely on providing information as the primary mechanism for ensuring informed consent. Studies have shown that users rarely read or understand lengthy privacy policies, and even when they do, cognitive limitations hinder their ability to make fully rational decisions.<sup>47</sup> Consequently, the effectiveness of disclosure as a regulatory tool is fundamentally limited.

Instead, regulation must focus on the context and architecture of choice, recognizing that how choices are presented is as important as the choices themselves. This involves scrutinizing interface designs that exploit default settings, obscure alternatives, or create artificial urgency.<sup>48</sup> Consent should not be considered valid where it is obtained through manipulative design practices that undermine user autonomy. In this sense, the emphasis shifts from whether consent was given to how it was obtained.

Another important dimension of rethinking consent is the introduction of substantive standards of fairness. Rather than relying solely on individual decision-making, regulators can impose obligations on firms to ensure that their practices do not exploit cognitive vulnerabilities.<sup>49</sup> This approach aligns with emerging trends in jurisdictions such as the European Union, where

---

<sup>44</sup> Harry Brignull, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* 120–135 (2023).

<sup>45</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1.

<sup>46</sup> Cass R. Sunstein, *Sludge Audits*, 12 BEHAV. PUB. POL'Y 1, 6–12 (2022).

<sup>47</sup> Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* 45–60 (2021 ed.).

<sup>48</sup> Organisation for Economic Co-operation and Development (OECD), *Dark Commercial Patterns* 41–45 (2022), <https://www.oecd.org>.

<sup>49</sup> Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 200–210 (2021).

regulatory frameworks increasingly emphasize fairness, transparency, and accountability in digital design. It also calls for greater integration of legal compliance within corporate governance structures, ensuring that ethical considerations are embedded in product development processes.

Furthermore, a behavioural-legal framework highlights the importance of ex ante interventions, such as design regulations, nudging standards, and algorithmic audits, which aim to prevent manipulation before it occurs.<sup>50</sup> These measures shift the regulatory focus from reactive enforcement to proactive governance, better suited to the dynamic nature of digital markets.

Ultimately, rethinking consent requires a departure from the idealized notion of the rational consumer toward a more realistic understanding of human behaviour. By integrating legal principles with behavioural insights, it becomes possible to develop a more robust and effective framework for protecting consumer autonomy in the digital age. Such an approach not only addresses the limitations of existing consent models but also lays the foundation for more ethical and accountable digital ecosystems.

## VIII. RECOMMENDATIONS AND SOLUTIONS

Addressing the challenges posed by dark patterns requires a shift from fragmented and reactive regulation toward a more integrated framework that combines legal reform, behavioural insights, and corporate accountability. Given that manipulation in digital markets operates at the level of design and psychology, solutions must extend beyond traditional disclosure-based approaches and focus on restructuring the architecture of choice itself.<sup>51</sup>

At the regulatory level, there is a pressing need for clear and enforceable definitions of dark patterns within statutory frameworks. While recent guidelines in jurisdictions such as India have begun identifying specific categories of manipulative practices, these must be codified into binding law with well-defined thresholds for liability.<sup>52</sup> Ambiguity allows firms to operate within legal grey areas, often justifying manipulative practices as legitimate business strategies. A standardized taxonomy of prohibited design practices, such as forced consent, subscription traps, and interface interference would provide greater clarity for both regulators and businesses.

In addition to definitional clarity, stronger enforcement mechanisms and penalties are essential.

---

<sup>50</sup> Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* 165–180 (2021).

<sup>51</sup> Cass R. Sunstein, *Sludge Audits*, 12 BEHAV. PUB. POL'Y 1, 12–18 (2022).

<sup>52</sup> Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns*, 2023 (India).

Regulatory authorities must be equipped with adequate technical expertise and resources to monitor complex digital environments.<sup>53</sup> This includes the ability to conduct audits of user interfaces, algorithms, and data flows. Penalties for non-compliance should be proportionate to the scale of harm and the economic benefits derived from manipulative practices, ensuring that violations are not treated as mere costs of doing business.

A critical component of reform lies in the adoption of design-based regulation, which focuses on preventing manipulation at the source. Rather than relying solely on user consent, regulators can mandate fair design standards that prioritize transparency, symmetry of choice, and ease of opting out.<sup>54</sup> For example, consent interfaces should present options in an equally prominent and accessible manner, avoiding the use of misleading colours, layouts, or default settings. Such measures shift the burden from users to firms, recognizing that individuals cannot reasonably be expected to navigate complex and strategically designed environments.

From a managerial perspective, organizations must integrate ethical considerations into corporate governance structures. Decisions related to user experience design should not be driven solely by performance metrics such as engagement or conversion rates but should also incorporate legal and ethical risk assessments.<sup>55</sup> Establishing internal review boards or ethics committees can help ensure that product development aligns with both regulatory requirements and broader societal expectations. This approach fosters a culture of responsible innovation, where long-term trust and reputation are valued alongside short-term profitability.

Another important recommendation is the implementation of algorithmic accountability and auditing mechanisms. As digital platforms increasingly rely on automated systems to optimize user interactions, it becomes essential to ensure that these systems do not perpetuate or amplify manipulative practices.<sup>56</sup> Independent audits and transparency requirements can provide oversight, enabling regulators and stakeholders to assess the impact of design choices on user behaviour.

Finally, consumer awareness and digital literacy must be strengthened as complementary measures. While regulation plays a central role, empowering users to recognize and resist manipulative practices can enhance the overall effectiveness of legal frameworks.<sup>57</sup> Educational

---

<sup>53</sup> Organisation for Economic Co-operation and Development (OECD), *Dark Commercial Patterns* 50–58 (2022), <https://www.oecd.org>.

<sup>54</sup> Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 210–220 (2021).

<sup>55</sup> Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* 180–195 (2021).

<sup>56</sup> Shoshana Zuboff, *The Age of Surveillance Capitalism* 210–230 (updated ed. 2021).

<sup>57</sup> Sinan Aral, *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health—and How We Must Adapt* 200–215 (2021).

initiatives and public awareness campaigns can help individuals better understand how digital interfaces influence their decisions, reducing their vulnerability to exploitation.

In sum, addressing dark patterns requires a multi-layered approach that combines legal reform, proactive regulation, corporate responsibility, and user empowerment. By aligning legal standards with behavioural realities and embedding ethical considerations within business practices, it is possible to create a more balanced digital ecosystem that protects consumer autonomy while allowing for innovation and growth.

## IX. CONCLUSION

The evolution of digital markets has fundamentally reshaped the meaning and operation of consent, exposing the limitations of traditional legal frameworks that rely on assumptions of rational and informed decision-making. This paper has demonstrated that in contemporary digital environments, consent is increasingly “*manufactured*” through the strategic use of dark patterns, design techniques that exploit cognitive biases, decision fatigue, and behavioural tendencies to influence user choices. What appears, on the surface, to be voluntary agreement often conceals a deeper structure of psychological manipulation, raising serious concerns about the integrity of consumer autonomy.

By examining the intersection of law, psychology, and management, the analysis highlights that dark patterns are not merely isolated instances of unethical design but are embedded within broader corporate strategies aimed at maximizing engagement, data extraction, and profitability. These practices are reinforced by competitive market pressures and enabled by technological capabilities that allow firms to continuously refine and optimize user influence. As a result, manipulation becomes systemic rather than incidental, challenging the adequacy of regulatory approaches that focus narrowly on deception or misrepresentation.

The legal frameworks currently governing digital markets, both in India and globally, have made important strides in recognizing the risks posed by manipulative design practices. However, they remain constrained by conceptual and practical limitations, particularly their reliance on formalistic notions of consent and reactive enforcement mechanisms. The persistence of ambiguity between permissible persuasion and unlawful manipulation, coupled with difficulties in proving harm and intent, allows dark patterns to operate within regulatory grey areas. This underscores the need for a more nuanced and proactive approach to consumer protection.

A central insight of this study is that effective regulation cannot be achieved without integrating behavioural realities into legal standards. The shift from formal consent to substantive

autonomy requires a reorientation of legal thinking, one that acknowledges the ways in which digital environments shape and constrain individual choice. This entails not only redefining consent but also reconfiguring the responsibilities of corporations, placing greater emphasis on ethical design, transparency, and accountability.

At the same time, the role of management is crucial in bridging the gap between legal compliance and ethical practice. Organizations must move beyond viewing regulation as a constraint and instead recognize the long-term value of trust, fairness, and responsible innovation. Embedding behavioural awareness within corporate governance structures can help mitigate the risks associated with manipulative design, aligning business objectives with societal expectations.

Ultimately, the challenge of regulating dark patterns reflects a broader transformation in the nature of power within digital economies. Control is no longer exercised solely through explicit rules or coercion but through the subtle shaping of choices and behaviours. Addressing this challenge requires an interdisciplinary approach that combines legal reform, psychological insight, and managerial responsibility. Only by confronting the underlying mechanisms of influence can legal systems effectively safeguard consumer autonomy and ensure that the digital marketplace remains both innovative and just.

\*\*\*\*\*