Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.12 n.57, p. 43-58. January/February, 2026.

DOI: https://doi.org/10.5935/jetia. v12i57.2715

ISSN ONLINE: 2447-0228

RESEARCH ARTICLE OPEN ACCESS

DARK PATTERNS IN DIGITAL DESIGN: A REVIEW AND ASSESSMENT VIA RISK, TRUST AND DIVERSITY SCORES

Preeti Marwaha[1], Shalu Mahajan[2], Ishitva Joshi[3], Kriti Mishra[4], Ananya[5], Priyanka Sharma[6] and Arunita Chaukiyal[7]

[1, 2, 3, 4, 5, 6, 7]Department of Computer Science, Acharya Narendra Dev College, University of Delhi, New Delhi-110019, India.
[2]Department of Commerce, Acharya Narendra Dev College, University of Delhi, New Delhi-110019, India.

[1]https://orcid.org/0009-0000-7425-4749, [2]https://orcid.org/0009-0004-0591-5995, [3]https://orcid.org/0009-0002-8841-1295
[4]https://orcid.org/0009-0006-7957-3558, [5]https://orcid.org/0009-0005-4234-1174, [6]https://orcid.org/0009-0009-3341-6823
[7]https://orcid.org/0009-0008-5185-5945

Email: preetimarwaha@andc.du.ac.in, shalumahajan@andc.du.ac.in, ishitvajoshi@outlook.com, kritimisra87@gmail.com, itsmeanayasrivastava@gmail.com, priyankasharma@andc.du.ac.in, arunita@andc.du.ac.in

ARTICLE INFO

Article History
Received: September 22, 2025
Revised: November 20, 2025
Accepted: January 1, 2026
Published: January 31, 2026

Keywords:
Dark Patterns,
Deceptive Patterns,
Trust,
Risk,
Diversity.

ABSTRACT

Digital platforms increasingly shape everyday life, yet their design choices often undermine consumer welfare using dark patterns which are deceptive interfaces that manipulate users' decisions. These practices, ranging from hidden costs in e-commerce to manipulative cookie consent prompts and obstructive subscription cancellations, compromise user autonomy and impose financial, privacy, and psychological harms. The risks vary in severity and reversibility, with some patterns leading to lasting detriment while others create cumulative burdens over time. Beyond immediate harm, dark patterns erode trust in digital systems by fostering frustration, skepticism, and disengagement, weakening the long-term relationship between consumers and platforms. Their persistence reflects strong incentives tied to short-term business metrics such as conversions and sign-ups, combined with weak regulatory oversight. Notably, the diversity of dark patterns like urgency cues, obfuscation, misdirection, and coercion etc. illustrates both their adaptability and the challenges of detection. This paper reviews the dark patterns on digital platforms and proposes a structured framework to evaluate dark patterns across three dimensions: risk, trust erosion, and diversity. It also explores mitigation strategies through fair design, transparency, and accountability, while considering the ethical and legal responsibilities of digital platforms. By centering the analysis on consumer trust and risk, the study highlights the pressing need for robust safeguards to counteract diverse manipulative designs and protect users in digital ecosystems.

I. INTRODUCTION

Trust is a foundational element of user engagement within digital environments, influencing behaviors across e-commerce, social media, mobile applications, and voice interfaces. Users depend on the assumption that digital platforms operate in good faith, offering clarity, protecting user interests, and fostering informed choices [1][2]. This trust is not only technical but also social and psychological, shaped by interface design, past user experiences, and perceived transparency [3]. When systems behave predictably, provide honest feedback, and respect user autonomy, users are more inclined to share data and develop sustained platform relationships [4]. However, this trust is increasingly jeopardized by the widespread use of deceptive interface strategies known as dark patterns, manipulative design tactics that coerce users into unintended actions such as sharing personal data, consenting to cookies, or subscribing without awareness [5]. These practices often emerge when business objectives, such as maximizing engagement or revenue, override ethical concerns [6]. Designers may justify such tactics under commercial pressure, even when user autonomy and welfare are compromised [7]. A common example includes cookie banners that visually emphasize "accept all" options or use misleading phrasing to steer user decisions, undermining genuine consent and eroding trust over time [8]. This erosion can fuel user skepticism, platform backlash, and broader

resistance against the digital economy and its governance mechanisms [9]. Critically, distinguishing between authentic trust and what scholars' term "fake trust", trust that is artificially constructed through manipulation or misrepresentation, is necessary for safeguarding user agency [10]. Fake trust may be built through false information, deceptive designs, or persuasive tactics that blur the line between autonomy and coercion [11]. In response to these challenges, the fields of Human-Computer Interaction (HCI), law, and AI ethics have begun developing systematic frameworks to detect, classify, and regulate dark patterns [12]. This interdisciplinary effort seeks to realign digital systems with principles of fairness, transparency, and user-centered design, advancing legal, technical, and ethical safeguards to ensure digital environments which genuinely respect user autonomy [13][14]. Dark patterns are the interface design strategies that deliberately manipulate, coerce, or mislead users into making choices that are not in their best interest, have become a central concern in the fields of human-computer interaction, design ethics, and digital regulation [15].

Coined by Brignull in 2010, the term originally described deceptive design techniques in user interfaces that were used in specific situations to manipulate user behavior and increase actions like sign-ups, purchases, or other forms of conversion. However, over the past decade, these practices have grown in sophistication and scale, evolving into systematic, pervasive design patterns that exploit cognitive biases and information asymmetries [16]. Today, dark patterns are embedded across a wide range of digital environments, including e-commerce websites that use countdown timers or hidden costs [17], mobile applications that obscure data deletion options [18] , social media platforms that employ infinite scrolls and manipulative notification systems [19], and even newer domains such as voice assistants, digital games, augmented reality (AR), and extended reality (XR), where manipulation can be more immersive and less visible to users [20]. As public awareness and regulatory scrutiny have grown, dark patterns have attracted multidisciplinary scholarly attention, from computer science, law, behavioral psychology, and design ethics. This literature review provides a thematically structured synthesis of the current academic and technical discourse surrounding dark patterns. Specifically, it maps the research landscape across six key domains:

1. **Foundational Work and Taxonomy Development**: These classify dark patterns by intent, technique, and impact, guiding ethical design and regulatory understanding.
2. **Application Domains of Dark Patterns**: Dark patterns are expanding into emerging technologies like voice interfaces, extended reality (XR), and AI-driven systems. These contexts introduce new manipulation risks such as misleading voice prompts, immersive consent traps, or biased AI recommendations, making detection harder. As interfaces evolve, so must ethically design standards to safeguard user autonomy and trust.
3. **Automated Detection of Dark Patterns**: Detection of deceptive design uses machine learning and UI analysis to identify manipulative interface elements. ML models analyze visual layouts, text, and user behavior, while UI analysis applies heuristics and design audits. Together, they reveal patterns that undermine user trust, agency, and experience, supporting efforts toward ethical and transparent design.
4. **Mitigation strategies for dark patterns**: Mitigation strategies for dark patterns include enforcing stricter regulations, ensuring transparent design practices, adopting ethical UX guidelines, and conducting regular audits. Educating users to recognize manipulative tactics, empowering them with clearer choices, and promoting accountability among organizations also reduce risks. Collaboration between policymakers, designers, and watchdogs strengthens long-term protection.
5. **Legal and ethical Analysis**: Deceptive design tricks users, damages trust, limits control over choices, and creates stress, resulting in harmful and unethical digital experiences. These target dark patterns through data protection laws like the General Data Protection Regulation (GDPR) in the European Union, California Consumer Privacy Act (CCPA), and Digital Personal Data Protection Act (DPDP) in India. These frameworks mandate transparency, informed consent, and user control to ensure ethical, user-centric digital experiences and protect privacy.
6. **Methodology for calculating metrics (Risk score, Trust Score and Diversity Score)**: Risk Score evaluates probability and impact of negative outcomes using weighted factors. Trust Score measure's reliability, compliance, and transparency via normalized indicators. Diversity Score quantifies representation across categories using Shannon Entropy.

To trace how Dark Pattern research has evolved, we generated a Storyboard Timeline figure from Scopus bibliometric data (as shown in figure 1 and figure 2) using python. Titles, abstracts, and author keywords were text-mined using curated dictionaries for the major themes: Types, Detection, Mitigation, Psychological Impacts, Ethics/Regulation, and scoring metrics. For each year, we calculated the proportion of publications mentioning these themes and plotted them as continuous lines with annotations that narrate the storyline. The results reveal a clear progression: research initially emphasized defining and categorizing Dark Pattern types, then shifted toward building detection methods, and more recently has begun exploring mitigation strategies. On the psychological–ethical/regulatory–metrics axis, early work focused on user psychology, followed by a growing body of studies addressing ethics and legal regulation, while metrics such as trust, diversity, and risk scores remain only sporadically represented. Taken together, the storyboard timelines show a maturing field that is moving from descriptive taxonomies, through diagnostic tools, toward prescriptive interventions—yet they also highlight mitigation practices and standardized evaluation metrics as key gaps for future research.

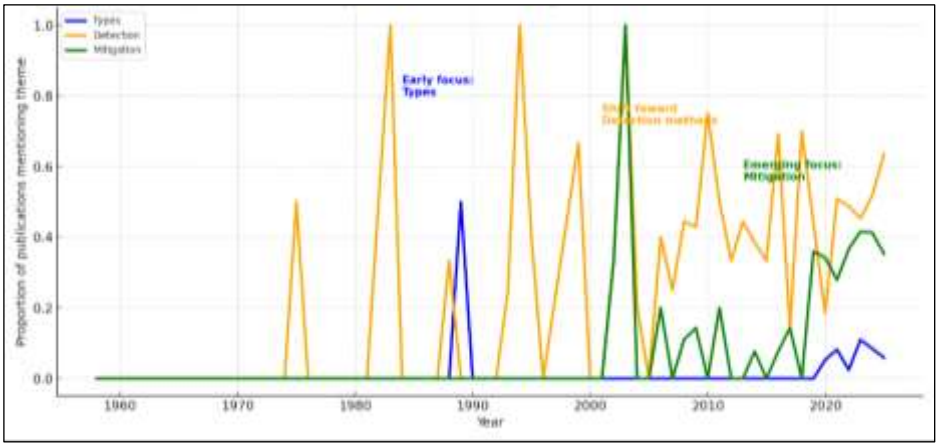

Figure 1: Storyboard Timeline-Types, Detection and Mitigation in Dark Patterns Research.
Source: Authors, (2026).

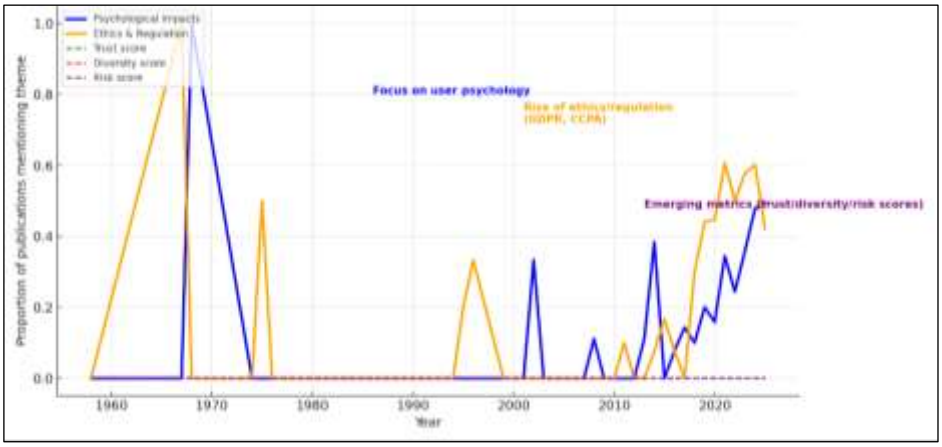

Figure 2: Storyboard Timeline-Psycological, Ethics/Regulation and Metrics in Dark Patterns Research.
Source: Authors, (2026).

II. FOUNDATIONAL WORK AND TAXONOMY DEVELOPMENT

The research around dark patterns revolve around designs that trick users into doing things they might not want to do, like giving up private information or making a purchase. It began with efforts to define and organize them into categories. Two landmark contributions in this area are the works of Gray et al. [5][6] and Gunawan et al. [22]-[21], both of which laid important foundations for understanding and detecting dark patterns in real-world user interfaces. Gray et al. conducted a seminal empirical study that examined real-world user interfaces to identify recurring manipulative design tactics. Their typology was grounded in a qualitative, ethnographic analysis and highlighted the psychological impact of these patterns on user autonomy. Gray et al.'s contribution was foundational, in establishing an ethical lens to assess dark patterns, emphasizing their capacity to erode user trust and agency. Building upon this framework, Gunawan et al. provided one of the most comprehensive classification systems to date. Their research extended the scope beyond web interfaces to include mobile platforms, highlighting the adaptability of dark patterns across different contexts. Their work focused on the structural features of dark patterns and their economic motivations, contributing a more systematic and platform-aware perspective. Zagal et al. [23]-[22] explored how video games use similar tricks like making players spend money to win and showed that these patterns can also appear in entertainment systems. Beyond simply listing and testing these patterns, other researchers have focused on their ethical implications. Devarmani et al. [7] argued that dark patterns aren't just annoying but unfair and morally wrong. They compared them to "nudges" (a term from behavioral science) that push people toward certain decisions in unethical ways. These researchers believe that dark patterns reduce people's freedom to choose and make online experience manipulative, which raises serious concerns about design responsibility and user rights. Table 1 gives the classification of Dark Patterns.

Table 1: Classification of Dark Patterns.

Category	Definition	Techniques / Subtypes	Examples
Information Concealment	Techniques that obscure, hide, or delay the presentation of key information from users, often encourage uninformed decisions.	• Hidden Information • Obfuscation • Alphabet Soup	• Amazon hiding subscription details under interface layers [21]-[23] • Legal/financial information buried in privacy policies [24] • Legalese/acronyms in Term and conditions [5]

Manipulative Wording or Design	Language and visual styles designed to mislead or hide true intent.	• Trick Questions • Misleading Reference Pricing	• Checkbox: "Uncheck this box if you do not want emails" [15] • Inflated original prices to simulate discounts [7]
Choice Architecture Exploitation	Structuring options which manipulate users into making specific, often suboptimal, decisions.	• Preselection • Drip Pricing	• Pre-ticked subscription/ product add-ons [16] • Fees revealed only at final checkout [5]
Coercive Design	Use of emotional pressure or psychological tactics to compel users to act.	• Forced Action • Nagging • Emotional Appeals Urgency	• Provide personal info or accept cookies to proceed [25] • Repetitive exit prompts [26] • "You'll make your cat sad…" [9]. Fake countdown timers [17]
Obstruction	Designs that intentionally make it difficult or time-consuming to take actions against the platform's interests.	• Complete Obstruction • Temporary Obstruction	• Multi-step or call-only cancellations [9] • Privacy settings buried in menus [27]
Sneaking	Actions are performed on behalf of the user without explicit consent or awareness.	• Hidden Costs • Disguised Ads • Drip Pricing • Manipulated Fairness Perception	• Add-ons like insurance, donation preselected [16] • Sponsored content disguised as native posts [5] • Sequential surcharge disclosure [28] • Manipulated Fairness Perception involves designing pricing or presentation tactics that make unfair or inflated costs seem reasonable [29]
Social Proof and Scarcity	Using real or simulated peer activity or limited availability to pressure decision-making.	• Low Stock Claims • Recent Purchase Alerts	• "Only 1 room left!"—often fake [27] • "Maria from London just bought this [17]
Social Engineering	Leverages psychological tricks and peer influence to manipulate behavior.	• Scarcity Claims • Social Proof • Shaming • Countdown Timer • Activity Messages • Fear of Missing Out (FOMO) • Friction in Account Deletion	• Scarcity Claims: "Only 2 left in stock!" to pressure purchases. • Social Proof: "500 people bought this today!" • Shaming: Labels like "No thanks, I prefer to pay full price." • Activity Messages: Fake updates like "Jessica just bought this". • Countdown Timers: Create urgency even if not real.
Gamification	Use of game elements to encourage repetitive use or spending.	• Pay-to-Play • Grinding • Countdown Ads • Infinite Scrolling • Addictive Design • Compulsion Loops • Reduced Friction to Keep Playing/Paying • Artificial Scarcity • Fear of Missing out (FOMO) • Power Imbalance via Purchases • Escalating Rewards • Anticipatory Triggers • Loot Box Rewards • Reward Saturation • Friction in Account Deletion • Bright Patterns Replacement	• Pay-to-Play: Must spend money to progress. • Grinding: Repetitive tasks required for minor rewards. • Countdown Ads: Must watch full ads before proceeding. • Infinite Scrolling: No stopping point to encourage endless use. • Addictive Design: Features like pull-to-refresh or reward loops. • Compulsion loops: Repetitive gameplay cycles that exploit rewards and anticipation to keep players engaged. • Reduced Friction to Keep Playing/Paying: Design choices that minimize obstacles, encouraging seamlessness, continuous engagement and spending without reflection. • Artificial Scarcity: Time-limited Rewards • Escalating Rewards: Rewards increase in value or rarity the longer or more frequently a player engages, encouraging prolonged play and repeated investment. • Anticipatory Triggers: Cues or signals (like animations or sounds) build excitement before rewards, manipulating players' anticipation to boost engagement and spending. • Loot Box Rewards: Randomized Rewards [30]

			• Reward Saturation: Overexposure to frequent in-game rewards diminishes their perceived value, leading players to seek increasingly intense stimuli to stay engaged [31] • Friction in Account Deletion: Deliberate obstacles like hidden settings, multiple confirmations, or delays or making deleting accounts difficult, users discouraged from leaving a platform or game [32] • Bright Patterns Replacement: Substituting transparent, user-friendly defaults for dark-patterned UI elements such as visible opt-outs, clear labels, and honest nudges [33]
Forced Action	Forces users to complete specific actions to access features or proceed.	• Forced Continuity • Forced Registration • Privacy Zuckering • Friend Spam • Granting permissions and Exploiting Interaction flows	• Forced Continuity: Free trials that auto-renew without clear notice. • Forced Registration: Must sign up before browsing content. • Privacy Zuckering: Pushing users to share more data than necessary [34] • Friend Spam: Encouraging users to spam contacts or share invites [35] • Granting permissions and Exploiting Interaction flows: Requiring excessive permission to use a service.
Interface Interference	Manipulates visual hierarchy, wording, or layout to mislead users.	• False Hierarchy • Bad Defaults • Visual Prominence • Small or Moving Close Button • Trick Questions	• False Hierarchy: Highlights or enlarges options like “Accept All”. • Bad Defaults: Pre-selected options benefit the service provider. • Visual Prominence: Important choices are visually downplayed. [36] • Small or Moving Close Button: Makes it hard to close pop ups or ads. • Trick Questions: Confusing language in opt-in/opt-out options. [37]

Source: Authors, (2026).

III. APPLICATION DOMAINS OF DARK PATTERNS

As dark patterns have proliferated across digital ecosystems, research has increasingly focused on specific domains where manipulation is especially pervasive or impactful. Thematic analyses reveal that deceptive design strategies often evolve in tandem with platform-specific affordances, regulatory gaps, and commercial incentives. This section synthesizes findings across four major application areas: e-commerce and consent interfaces, mobile applications, social media platforms, and emerging modalities such as XR, voice interfaces, and games.

A. E-Commerce and Consent Interfaces

Dark patterns, specifically deceptive interface designs, are widely studied in e-commerce platforms due to their direct influence on consumer behavior and revenue generation. These platforms often deploy manipulative tactics such as hidden fees, urgency cues, misleading CTAs, and forced choices to increase conversions and secure consent while undermining transparency and user autonomy. Research on dark patterns highlights widespread manipulative design practices across digital platforms. Singh et. al. [38] audited Indian e-commerce platforms while Chaudhary et. al. [39] studied other E-commerce platforms and found urgency cues (“Only 1 item left!”), misdirection with prominent “Buy Now” buttons, and hidden fees at checkout, exploiting attention limits, creating artificial scarcity, and undermining transparency. Nouwens et al. [8], in a large-scale analysis of EU websites, identified pre-checked boxes, confusing language, and visually dominant “Accept All” buttons in cookie consent banners, showing that consent is manipulated rather than freely given.

Similarly, Santos et al. [40] examined web privacy interfaces and revealed deceptive layouts and text mimicking privacy tools while nudging consent, again demonstrating consent manipulation. Berens et al. [41] analyzed cookie disclaimers, identifying obscured opt-out paths and visual hierarchies favoring acceptance, which subvert informed consent and reduce transparency. Vishvakarma et al. [42] applied Agency Theory to e-commerce platforms, noting deception for profit, conflicts between business incentives and user interests, and information asymmetry that benefits platforms over users. Experimental evidence further illustrates these effects: Santana et al. [43] showed consumers often choose lower base-price options but end up paying more when hidden fees are added through drip or partitioned pricing and anchoring bias exploitation; although transparency reduces the effect, biases persist. Fecher [44] found that later disclosure of surcharges in travel-booking reduces perceived value and trust, particularly for price-conscious consumers, with drip pricing and hidden fees undermining brand trust and purchase intent. Moriuchi et al. [29] studied peer-to-peer lodging platforms like Airbnb,

showing that drip pricing, hidden fees, and manipulated fairness perceptions reduce consumer trust and intent when fees seem deceptive, though transparent pricing can lessen backlash. Finally, Ahmetoglu et al. [45] reviewed behavioral pricing tactics, finding that anchoring bias, partitioned pricing, drip pricing, and price obfuscation distort consumer choice, obscure total costs, reduce transparency, and raise ethical concerns about fairness in marketing. Together, these studies underscore how dark patterns exploit cognitive biases, manipulate consent, and erode consumer trust across contexts.

B. Mobile Apps and OTT Platforms

Mobile platforms introduce unique challenges for dark pattern detection and user experience due to small screen sizes, touch-based interaction, and app-centric ecosystems. These constraints are often exploited to hide options, obscure data deletion, or create misleading pathways. Dark patterns manifest differently across platforms and interfaces, often exploiting either consent, data, subscriptions, or interaction through manipulative navigation and behavioral nudges. Gunawan et al. analyzed cross-platform environments and identified bait and switch, hidden costs, forced continuity, and nagging, noting that limited mobile screen space intensifies hidden costs, preselection, and obfuscated opt-outs, disproportionately affecting users with cognitive or motor impairments. Ramteke et al. examined mobile apps and found friction in account deletion, misleading opt-out buttons, and covert data sharing practices; in freemium models, these deceptive designs drive retention while undermining informed consent and user control over data.

Similarly, Chen et al. used the AppRay tool to detect structural manipulation in app navigation, such as circular menus, disappearing back buttons, and trapped exit paths, showing how subtle UI designs hinder user autonomy and resist regulation. Ramokapane et al. [46] focused on data deletion workflows in mobile apps, uncovering multi-step deletion processes, non-intuitive instructions, and lack of confirmation or feedback, raising serious concerns about resistance to user data rights. In subscription contexts, Nguyen et al. [47] in his case study and Ye et al. [48] found that music streaming platforms like Spotify and Apple Music deploy auto-renewal defaults, friction in cancellation, and habit reinforcement loops, which promote lock-in, reduce autonomy, and influence behavior.

Oyibo et al. [49] investigated awareness of dark patterns in streaming sites such as YouTube and Ivysci, showing that users without knowledge are more susceptible to confirmshaming and trick questions (68% compliance), while awareness reduces compliance to 35%, indicating transparency and education mitigate manipulation and protect platform reputation. Nygren et al. [50] inspected interfaces across YouTube, Netflix, Disney+, and Prime Video, reporting widespread forced continuity, hidden subscription costs, invasive mobile pop-ups, manipulative cookie-consent defaults, and autoplay loops, underscoring the need for regulatory scrutiny and industry audits. Rhomberg et al. [51] and Alashwali et al. [52] emphasized interventions to empower users through tools like browser extensions, educational guides, and transparency features, proposing “bright patterns” such as auto-renewal toggles and clear consent mechanisms to reduce susceptibility.

Extending beyond traditional UI, Mattiuzzo et al. [53] showed that TikTok leverages personalization and design nudges algorithmic sequencing, timing controls, and personalized content loops to influence retention, sometimes overriding user intent, while Dubiel et al. [54] highlighted how enhanced voice fidelity in conversational agents increases trust and compliance even with misleading suggestions, making vocal manipulation a novel non-visual dark pattern that requires ethical regulation. Finally, Franzen et al. [55] explored UX practitioners’ perspectives, revealing that many rationalize privacy-related dark patterns such as default opt-ins, deceptive toggles, and coercive consent designs as necessary trade-offs, highlighting the urgent need for stronger ethical standards, designer training, accountability mechanisms, and regulation around privacy defaults.

C. Social Media and Engagement Loops

Social media platforms are designed around continuous engagement, and as such, they often employ dark patterns that target psychological vulnerabilities to maximize time-on-platform. These manipulations are deeply embedded in algorithmic curation, notification design, and interface dynamics. What distinguishes dark patterns in this domain is their temporal and psychological nature: rather than misleading a user once, they shape ongoing behavior, subtly steering attention and habit formation over time. This raises complex ethical issues, especially for younger users and vulnerable populations. Research on social media platforms shows how design patterns exploit psychological vulnerabilities to maximize engagement, often at the cost of user well-being and autonomy. Beltrán et al. [56] and Clark et al. [57] highlighted how infinite scroll, intermittent rewards such as variable likes, autoplay, and disappearing content create compulsive engagement loops, mirroring gambling mechanisms that exploit variable-ratio reinforcement.

These patterns reduce user well-being, induce anxiety, undermining control, and raise serious ethical concerns over loss of agency. Extending this critique, Mamun et al. [58] and Ahuja et al. [59] argued that platforms deliberately prioritize engagement optimization and manipulative metrics over user autonomy or mental health. They called for systemic reforms, including greater transparency in engagement metrics and regular audits of design practices, to ensure alignment with ethical standards. Together, these studies emphasize how social media dark patterns particularly those rooted in interaction design and reinforcement mechanics erode informed choice, compromise user agency, and necessitate stronger accountability mechanisms.

D. XR, Voice Interfaces, and Game Design

Emerging modalities like extended reality (XR), voice assistants, and digital games introduce novel interaction paradigms that also expand the scope of dark pattern deployment. In these environments, manipulation often exploits spatial, auditory, or reward-based structures that differ from traditional screens. voice-based dark patterns rely on tone, timing, and control of dialogue flow rather than visuals. They exploit listening effort, memory limits, and social cues to manipulate users’ decisions. The evolution of interfaces expands the scope of potential manipulative practices, extending beyond screen-based interactions to encompass bodily gestures, spoken commands, and reward-based systems. They also signal a growing need for modality-specific detection frameworks, legal protections, and design guidelines. Supportive vs. Manipulative Tones in Voice Interfaces. Research on online gaming highlights how dark patterns in design exploit psychological mechanisms, often undermining fairness, autonomy, and player well-being. Freeman et al. [60] examined

competitive games, showing that pay-to-win mechanics and purchase-driven power imbalances erode perceived fairness, reduce trust, and heighten frustration in competitive contexts.

Larche et al. [61] analyzed loot box systems, finding that rare rewards trigger heightened arousal and encourage repeated openings, exploiting variable reinforcement schedules akin to gambling and fostering potentially addictive behaviors. Vulnerable groups such as adolescents with Internet Gaming Disorder (IGD) face intensified risks. Liu et al. [62] revealed that reduced loss aversion and inhibitory control make them more susceptible to compulsion loops and low-friction play/pay mechanics, while Raiha et al. [63] demonstrated altered neural reward processing, where escalating rewards and anticipatory triggers reinforce addictive cycles. Similarly, Zhou et al. [64] found that IGD individuals display heightened sensitivity to in-game over real-world rewards, amplifying reward saturation and reinforcing escapism. Beyond addiction, engagement mechanics can also pressure players. Frommel et al. [65] studied daily quests and incentives, showing how artificial scarcity and fear of missing out (FOMO) can sustain habitual engagement but also generate burnout or pressure-driven play. Together, these studies illustrate how gaming dark patterns, especially through compulsion loops, reinforcement schedules, and reward manipulation, exploit cognitive vulnerabilities to drive monetization and engagement, raising ethical concerns over fairness, player health, and industry responsibility.

IV. AUTOMATED DETECTION OF DARK PATTERNS

As dark pattern research matured, scholars increasingly turned their attention to automated detection techniques aimed at identifying deceptive designs at scale. These efforts span mobile applications, websites, e-commerce systems, and emerging platforms, reflecting growing concern over unethical user interface practices. Approaches can be broadly categorized into language-based, visual/UI-based, and structural/DOM-based methods. Together, these methods reflect a maturing research landscape seeking scalable, generalizable, and explainable solutions.

A. Language-Based Detection

Language-based detection methods harness natural language processing (NLP) and transformer models to uncover manipulative textual content embedded in interfaces. Salminen et al. [66] trained a RoBERTa model on retail scenarios to identify deceptive strategies like drip pricing and false urgency. Their system achieved high F1-scores (up to 0.969), and the use of explainable AI tools such as LIME and SHAP enabled the identification of linguistic markers like scarcity, popularity, or FOMO cues. Sazid et al. [67] extended this line of work using GPT-3 in a few-shot learning setting, showing its ability to classify dark patterns with minimal labeled data, highlighting its adaptability across domains. Similarly, Ramteke et al. combined BERT with a web scraping pipeline to detect urgency-based and misdirection patterns in e-commerce, achieving a 96% accuracy rate. These studies underscore the effectiveness of transformer-based models in decoding subtle cues of manipulation in text-heavy interfaces.

B. Visual and UI-Based Detection

Because many dark patterns rely on visual deception—such as hiding options, contrast manipulation, or misleading layout—visual and UI-based approaches have emerged to interpret interface structure beyond language. Kodmurgi et al. [68] applied YOLOv5, a real-time object detection algorithm, to Android app screenshots, accurately identifying UI components associated with deceptive design choices. Mansur et al. [69] introduced AidUI, a multi-modal architecture that integrates visual layout features, user interaction traces, and semantic understanding to detect manipulation in both web and mobile contexts. These models highlight the importance of interpreting *how* interface components are positioned, styled, and presented to users—particularly when visual tricks are used to nudge behavior. Tools like UIGuard combine computer vision with text recognition and rule-based classification. Their system, built with Faster R-CNN and PaddleOCR, was deployed on mobile interfaces and achieved 0.93 accuracy. It significantly improved users' dark pattern detection recall (from 18.5% to 57.8%), though it remained constrained when handling unfamiliar pattern types. Likewise, Kodandaram et al. designed a detection system for screen-reader accessibility, targeting deceptive ads that harm visually impaired users. Their model combined transformer layers, an LSTM module, and DOM-derived features for high-precision classification, representing an often-overlooked domain in mainstream detection tools.

C. Structural/DOM-Based Detection

This approach focuses on analyzing a webpage's underlying logic and element hierarchy, rather than just its visible content or appearance. Early systems relied on rule-based parsing of HTML to flag patterns like "sneaking" or "misdirection." While these methods work well for known dark patterns, they require frequent manual updates and lack adaptability to new designs. To address these limitations, Nie et al. introduced the *Dark Pattern Analysis Framework* (DPAF), which builds on a taxonomy-driven review of 76 core studies. DPAF identifies 64 dark pattern types—20 of them newly defined—and maps existing detection methods to this taxonomy. Their work highlights significant interoperability issues and the absence of automated updating mechanisms that could keep pace with evolving deceptive design strategies. In a more holistic direction, Stavrakakis et al. introduced a morphological matrix framework that combines HTML parsing, computational linguistics, and image analysis. Their prototype successfully flagged patterns across categories but still faced challenges with UI. A third major category focuses on interface structure, particularly the Document Object Model (DOM) used in web and app design. These methods investigate how manipulation is embedded in the hierarchy, logic, or flow of interface elements. Bajaj et al. [70] modeled DOM trees in mobile apps to detect coercive flows—such as hidden cancel buttons or misleading progress indicators—by analyzing navigation paths and element nesting. Mansur et al. addressed the challenge of cross-platform applicability, proposing a generalization framework to train models that can detect dark patterns across varying UI architectures and environments. Cookie banners, a frequent site of consent manipulation, have been extensively studied through Document Object Model (DOM) analysis. Vedhapriyavadhana et al. [71] introduced a multi-faceted system to detect dark patterns such as deceptive UI/UX practices in shopping websites using Bidirectional Encoder Representations from Transformers (BERT) and DOM.

It used a Chromium browser extension, a machine learning backend, and a companion website to identify manipulative design elements in real-time and highlights them for users. Hausner et al. [72] used Support Vector Machines (SVMs) to classify manipulative designs based on HTML structure, textual cues, and CSS styling, with a focus on contrast tricks (e.g., highlighting "Accept" while hiding "Reject"). Ramokapane et al. applied machine learning to cluster banner components, revealing difficulties with inconsistent layouts and labeling schemes that hamper automated classification. These findings suggest that deception often resides in the interval variability and inconsistent semantics, echoing the call for more flexible, resilient systems. Together, these detection approaches illustrate the field's shift toward scalable, data-driven solutions. While many tools reach high performance in controlled environments, a common limitation persists difficulty generalizing to novel, dynamic, or platform-specific dark patterns. Emerging strategies aim to bridge this gap using transfer learning, explainable AI, and cross-platform models, but success will depend on continuously updated datasets, taxonomies, and more user-centered tools that promote transparency and trust. Despite promising accuracy, real-world deployment of these systems remains limited.

D. Hybrid/Ensemble Approaches

This approach combines two or more of the above strategies to maximize coverage. For example, a system may use NLP for text cues and DOM parsing for structural clues. Kodmurgi et al. introduced *ScrapeAI*, a multi-modal architecture that combines UI screenshots, code structure, and behavioral logs to detect dark patterns with promising accuracy. Abraham et al. proposed three detection algorithms—rule-based, ML-based, and hybrid—which showed complementary strengths in various commercial settings. Its multi-modal nature improves detection accuracy but comes at high computational cost and deployment complexity. In contrast, Abraham et al. advocate a modular hybrid model that balances rule-based interpretability with machine learning generalization. Their approach is more adaptable but struggles with dynamic content. Together, these methods reveal a trade-off between specificity and scalability—a challenge that remains unresolved.

V. MITIGATION STRATEGIES FOR DARK PATTERNS

This area remains underdeveloped compared to advances in detection. While research has focused heavily on identifying manipulative designs, fewer efforts address how to actively counter or prevent them. User-facing interventions show some promise: Schäfer et al. [73] demonstrated that simple design adjustments such as overlays, clearer consent options, and standardized button hierarchies can reduce mis clicks and enhance agency. Similarly, Kronhardt et al. [74] introduced a gamified tool that trains users to recognize manipulative patterns, improving awareness and literacy, though such approaches remain experimental and largely absent from mainstream platforms. From a regulatory and industry perspective, proposals like Rana et al. [75] Legal UX Audits suggest that interface designs could undergo compliance reviews much like financial or security audits. This model shifts the focus from penalizing violations after the fact to proactively setting standards for acceptable design. Yet these ideas remain largely theoretical, with limited institutional adoption. Meanwhile, a major gap persists for developers and designers, who lack real-time ethical evaluation tools comparable to accessibility or performance checkers. Without such support, ethical UI design often depends on ad-hoc expertise or retrospective audits, which are inadequate in fast-moving development contexts. Overall, progress in intervention is fragmented. To move forward, research and practice must embed ethical toolkits into design workflows, establish regulatory sandboxes, build educational infrastructure for users and developers, and standardize protocols for UI evaluation. Without these measures, detection will continue to outpace deterrence, allowing manipulative practices to evolve unchecked.

VI. LEGAL AND ETHICAL ANALYSIS

The legal and ethical analysis of dark patterns shows both convergence and divergence across global and Indian contexts. Globally, scholars like Luguri et al. frame the issue around autonomy and coercion, with regulation focused on consent, cookie banners, and manipulative e-commerce practices. Reports such as the Norwegian Consumer Council's 2018 [76] study spurred EU and US inquiries, and while frameworks like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) set high standards, enforcement remains inconsistent. Studies indicate that platforms often practice strategic compliance rather than genuine design reform, leaving many forms of soft manipulation beyond effective legal reach. In India, by contrast, the framing emphasizes socio-technical vulnerability, reflecting the realities of mobile-first users, low digital literacy, and systemic inequities. The Consumer Protection Act (2019) [77] laid a broad foundation, but the 2023 "*Guidelines for Prevention and Regulation of Dark Patterns*" [78] marked a decisive step. It explicitly classifies manipulative practices and aligns with the Digital Personal Data Protection Act, emphasizing meaningful consent. Enforcement, however, is challenged by weak technical capacity, low consumer awareness, and fragmented oversight [79]. Ethically, the global debates stress autonomy and transparency, Indian discourse prioritizes digital equity, inclusive design, and protection for vulnerable users.

This comparison underscores that while the global approach leans on universal principles of autonomy, India advances a contextual, equity-driven model that addresses both cognitive and structural vulnerabilities [80]. Hence, combating dark patterns demands regulation, ethical design standards, user education, and metrics valuing long-term user welfare over short-term profit [81]. Even minor or small deceptive acts on digital platforms can erode trust [82]. Dark Patterns manipulate users' behavior, reduce autonomy, and undermine enjoyment, highlighting the urgent need for ethical, transparent design on various platforms [83]. Users still limit sharing sensitive data. Firms gain via better targeting, stronger marketing, and greater lock-in, showing regulation can protect privacy *and* support business outcomes [84][85][86]. Dark patterns continue to undermine consumer autonomy across domains such as e-commerce, gaming, and streaming. Hung (2021) highlights how "nagging" patterns create persistent consumer injury, while Li (2022) examines evolving regulatory responses under the FTC and CPRA to manipulative cookie consent notices. Few research focuses on remedies: Yao and Wei [87] propose improved terms-of-service design to reduce user confusion, whereas Singh, Vishvakarma, and Kumar [88] use grey influence analysis to study consumer challenges, and later authors in [89] show how deceptive design erodes brand equity. Zac et al. [90] stress that

consumer vulnerability magnifies harm, aligning with Bhoot et al. [91], who identify patterns through user reactions. Experimental evidence by Koh et al. [92] demonstrates how four common e-commerce dark patterns drive unintended consumption, while Nygren et al. document similar tactics in video streaming services. Parallel work on music streaming by Li, Liu, and Chen [93] underscores that user satisfaction and retention may be compromised by manipulative interfaces. Collectively, these studies suggest that dark patterns are not only prevalent but context-specific, raising urgent questions about ethics, user welfare, and regulatory oversight [94][95].

VII. METHODOLOGY

Step 1: Dataset Creation

A labeled dataset was created to examine 39 categories of dark patterns across widely used platforms. The categories include e-commerce (e.g., Amazon, Flipkart, Meesho, Myntra, Nykaa, Shopsy etc.), finance (Paytm, GPay etc.), gaming (Scribble.io, Minecraft etc.), matrimonial/dating/chatting (Instagram, whatsapp, Bhartmatrimony, Jeevansathi etc.), OTT (Netflix, Zee5, Amazon prime etc.), blockchain/cloud (AWS, GCP, casper, Blockchain.com etc.) and educational (Grammarly, W3 school and various universities) platforms. In this study, the unit of analysis was defined as an observable UI instance such as a text element, widget, flow step, or micro-interaction that exhibited or was suspected of exhibiting manipulative behavior (e.g., drip pricing, urgency cues, scarcity claims, or obstruction). To ensure comprehensive coverage, we examined key user flows across platforms, including the landing or homepage, sign-up and onboarding processes, the cart-to-checkout-to-pricing journey, cookie consent dialogs, settings and privacy options, as well as unsubscribe, refund, and cancellation mechanisms. These flows were tested across multiple user states namely, logged-out visitors, newly created accounts, returning users, and incognito sessions—to capture potential variations in dark-pattern deployment. A hybrid approach was employed, combining manual inspection of user flows with AI-assisted verification. Microsoft Copilot (Edge Sidebar) and Perplexity were used to extract UI text, summarize prompts, and flag potential dark patterns. Every AI prompt and output was logged for traceability, but manual verification remained mandatory to mitigate the risk of AI hallucinations and ensure the accuracy of identified instances.

A systematic process is followed to capture data to ensure consistency and reliability. For session setup, a Chromium-based browser (stable release) in both normal and private modes is used with cache and cookies cleared between sessions. The testing environment was configured to a desktop viewport ranging from 1366×768 to 1920×1080, set to the India locale with English as the default language. Only test accounts were created and used, with no personal data or payment details stored. For evidence collection, each candidate dark pattern was documented using multiple forms of data: screenshots and screen recordings captured before, during, and after user interactions; DOM snapshots that included visible text and relevant HTML snippets (via Inspect/Accessibility Tree); and, when necessary, network traces to verify whether timers or stock counters were dynamically fetched from the server or simply hard-coded and resettable. All captures were timestamped in ISO format to help detect recycled or false countdowns. These artifacts were stored in a structured directory hierarchy, with each session folder containing screenshots, recordings, DOM dumps, and notes for clarity and reproducibility. For AI-assisted review, Microsoft Copilot (Edge sidebar) and Perplexity were used as secondary verification tools. They extracted page text, summarized visible prompts, and suggested possible dark-pattern categories. However, their outputs were never accepted without manual confirmation, and any disagreements or vague categorizations were explicitly flagged as requiring manual adjudication. Candidate instances were assessed using objective and rule-based criteria to minimize subjectivity. A few examples are listed below in Table 2.

Table 2: Examples - Dark Patterns and their Trigger Rule.

Category	Objective	Decision Rule (Pass if…)	Example Triggers
Drip Pricing	Hidden fees, preselected add-ons	Material price element appears only after checkout initiation	“Convenience fee” at payment, gift wrap auto-selected
Urgency / Countdown	Timers, “ends soon” messages	Countdown persists across sessions or resets on reload	“Offer ends today” but reappears next day
Scarcity / Low Stock	“Only X left”	Stock claim static/unrealistic across refresh	“Only 1 left” on many SKUs
Social Proof / FOMO	“N people bought in 24h”	Unverifiable claims, often paired with urgency	“7,421 purchased today”
Disguised Ads	Sponsored content styled as organic	Paid content lacks equal disclosure	“Recommended” tiles w/o “Ad” tag
Friction in Deletion	Multi-step/hidden deletion	Requires >3 steps or off-platform action	“Email support to delete”
Forced Action	Pre-checked boxes, blocked progress	Opt-out harder to find/use than opt-in	“Yes, send me offers” checked by default
Hidden Costs	Late-stage fees	Non-optional fee not disclosed upfront	“Platform fee” added at last step

Source: Authors, (2026).

To evaluate candidate instances systematically, a set of rule checks was applied. The Equal-Prominence Test was used for consent-related choices, requiring that opt-out options carry comparable visual weight to opt-in options (at least 70% in size and positioned at the same panel depth). Failure to meet this criterion was marked as obstruction or misdirection. The Reset/Replay Test was applied to urgency and scarcity claims, where timers and stock counters were reloaded in fresh sessions; if these elements reset or behaved implausibly, they were flagged as false urgency or scarcity. Finally, the Click-Count Heuristic was used to evaluate cancellation flows, with subscribing allowed within two clicks but cancellations or deletions requiring four or more clicks or redirecting users off-platform are considered friction-inducing dark patterns.

Step 2: Cleaning of Dataset and Assigning weights using Saaty's AHP (Analytic Hierarchy Process)

For this study, a systematic data cleaning process was applied to ensure reliability and consistency of the binary dataset. First, all collected artifacts (screenshots, DOM snapshots, network traces, and notes) were cross-checked to confirm whether a dark pattern instance was genuinely present. Any ambiguous cases flagged by AI tools were manually reviewed and either validated or discarded to avoid false positives caused by hallucinated outputs. Duplicate records arising from repeated flows (e.g., refreshing pages or testing across user states) were identified and removed to prevent inflation of frequencies. Inconsistent labels across similar instances were standardized according to the predefined taxonomy of 39 dark-pattern categories, ensuring uniform coding. Finally, the binary encoding was verified where 1 consistently denoted the presence of a dark pattern and 0 denoted its absence, producing a clean and structured dataset suitable for pairwise comparison and AHP analysis. To construct the pairwise comparison matrix, the binary dataset was first interpreted. Each row represented an observation i.e., websites, webapps, mobile apps etc., belonging to different categories. Each column in the dataset corresponded to a criterion, such as Hidden Information, Obfuscation, Drip Pricing, Urgency, or Scarcity etc. Each criterion's frequency was then calculated as the number of rows in which it appeared (i.e., where the value equaled 1).

Using these frequencies, a reciprocal pairwise comparison matrix was generated, where the relative importance of criterion i over criterion j was defined as the ratio $a_{ij} = {f_i}/{f_j}$ where f_i and f_j represents frequencies of criterion i and j in the dataset. All diagonal elements (a_{ii}) are equal to 1 and $a_{ji} = {1}/{a_{ij}}$. The Saaty's Analytic Hierarchy Process (AHP) [96] is applied where the matrix was column-normalized, and the priority vector was computed as the row-wise average of the normalized matrix, yielding the relative weights w_i of each dark pattern. Finally, the consistency of the matrix was evaluated using AHP's consistency metrics. The largest eigenvalue λ_{max} was found to be 39.0 (equal to the number of criteria), leading to a Consistency Index (CI) of 0.0 and a Consistency Ratio (CR) of 0.0, indicating perfect consistency. This outcome was expected because the pairwise ratios were derived directly from observed frequencies, making the matrix mathematically transitive and free of contradictions, with the resulting weights directly reflecting the observed distribution of dark patterns in the dataset.

Step 3: Calculation of Risk Score, Trust Score and Diversity score using Weighted Shannon's Entropy Method

Trust Score, Risk Score, and Diversity Score of dark patterns across various categories in dataset are calculated using weighted Shannon's Entropy [97]. The algorithm begins by measuring the uncertainty of each criterion using equation 1 and equation 2. For every feature, Shannon entropy is computed by considering the distribution of its values across all records. Lower entropy indicates that the criterion provides more useful information, so it is transformed into an information utility measure by taking one minus the entropy value using equation 3. Next, it is combined with the Saaty AHP weights w_i computed in step 2. Each criterion's original weight w_i is multiplied by its information utility d_i and then normalized so that the adjusted weights sum to one. Using these adjusted weights w_i', the Risk Score for each row is calculated as the weighted sum of all the dark pattern indicators present, while the Trust Score is defined as one minus the Risk Score. Finally, the Diversity Score reflects the variety of dark patterns influencing each row and is computed as the Shannon entropy across that row's distribution of criteria. This way, Risk Score captures the intensity of dark patterns, Trust Score represents resilience against them, and Diversity Score measures how varied those dark patterns are within a given record.

To compute Trust Score (*TrustScore*), Risk Factor (*RiskScore*), and Diversity Score (*DiversityScore*) with Shannon entropy and AHP weights, with the dataset having m =40 rows (records) and n =39 criteria, with $x_{ij} \epsilon \{0,1\}$ indicating presence of criterion i in row j, and w_i is the AHP weight for criterion i , with $\sum_i w_i = 1$ calculated in step 2. The Shannon entropy of criterion i (normalized to [0,1]] for a binary variable) is given as equation 1:

$$H_i = -\left(\frac{1}{\ln(2)}\right)(p_i \ln(p_i) + (1 - p_i)\ln(1 - p_i)) \quad (1)$$

where p_i is calculated using equation 2 as:

$$p_i = \left(\frac{1}{m}\right)\Sigma_{j=1}^{m} x_{ij} \quad (2)$$

A small ε is used to replace any 0 inside logs if needed. The entropy is converted to information utility using equation 3 as:

$$d_i = 1 - H_i \quad (3)$$

The algorithm adjusts calculated weights using equation 4 to favor more informative criteria:

$$w_i' = \frac{(w_i * d_i)}{\sum_{\{k=1\}}^{\{n\}} w_{k^*} d_k} \quad (4)$$

Then the Risk score for each row i is the adjusted weighted sum of active criteria and is calculated using equation 5.

$$RiskScore_{\ i} = \sum_{i=1,j=1}^{m,n} w_j' * x_{ij} \quad (5)$$

The Trust Score for row i is calculated as complement of Risk Score using equation 6.

$$TrustScore_i = 1 - RiskScore_i \quad (6)$$

The Diversity Score for row i, is calculated using equation 7

$$.q_{ij} = \frac{\{x_{ij}\}}{\left\{\sum_{\{i=1\}}^{n} x_{ij}\right\};} \quad if \ \sum_{\{i=1\}}^{n} x_{ij} > 0$$
$$DiversityScore_i = -\left(\frac{1}{\ln(n)}\right) \sum_{j=1}^{n} q_{ij} \ln(q_{ij}) \tag{7}$$

The next section presents the analysis of results obtained after using above formulas on the dataset.

VII. RESULT ANALYSIS

The values of Risk Score (*RiskScore)*, Trust Score (*TrustScore)* and Diversity Score (*DiversityScore)* for our dataset are calculated using Shannon Entropy (weighted) method which uses Saaty's AHP for weight assignment. The analysis shows that e-commerce websites have the highest level of manipulation, with a very high *RiskScore* (~0.90) and very low *TrustScore* (~0.09). Their *DiversityScore* (~0.94) also suggests that they use wide variety of dark patterns, making them the most deceptive category overall. Educational websites present a more balanced picture, with a moderate *RiskScore* (~0.48) and a relatively higher *TrustScore* (~0.52). Their *DiversityScore* (~0.57) indicates that while some manipulative tactics exist, they are less frequent and less diverse compared to e-commerce. Finance platforms also show moderate levels, with *RiskScore* (~0.49) and *TrustScore* (~0.51) being almost evenly balanced. However, their *DiversityScore* (~0.73) suggests that financial platforms employ a broader set of manipulation techniques than educational sites, even if the overall risk is not excessively high.

Chatting and matrimonial/dating apps display a concerning profile, with a high *RiskScore* (~0.73) and a relatively low *TrustScore* (~0.27). Their *DiversityScore* (~0.87) highlights that they employ a large variety of dark patterns, making them one of the riskiest categories alongside e-commerce websites. Games are perceived far more positively, with a low *RiskScore* (~0.22) and a high *TrustScore* (~0.78). Their *DiversityScore* (~0.46) shows that although some manipulative designs exist (like loot boxes or addictive loops), they are relatively limited in range and intensity compared to other sectors. Finally, Blockchain and cloud platforms emerge as the safest and most trusted category. They have the lowest *RiskScore* (~0.18) and the highest *TrustScore* (~0.82) among all categories. Their *DiversityScore* (~0.37) indicates that they use very few dark patterns overall, reinforcing their perception as the least manipulative sector. These results are visualized using a heatmap and bar chart for different categories of website.

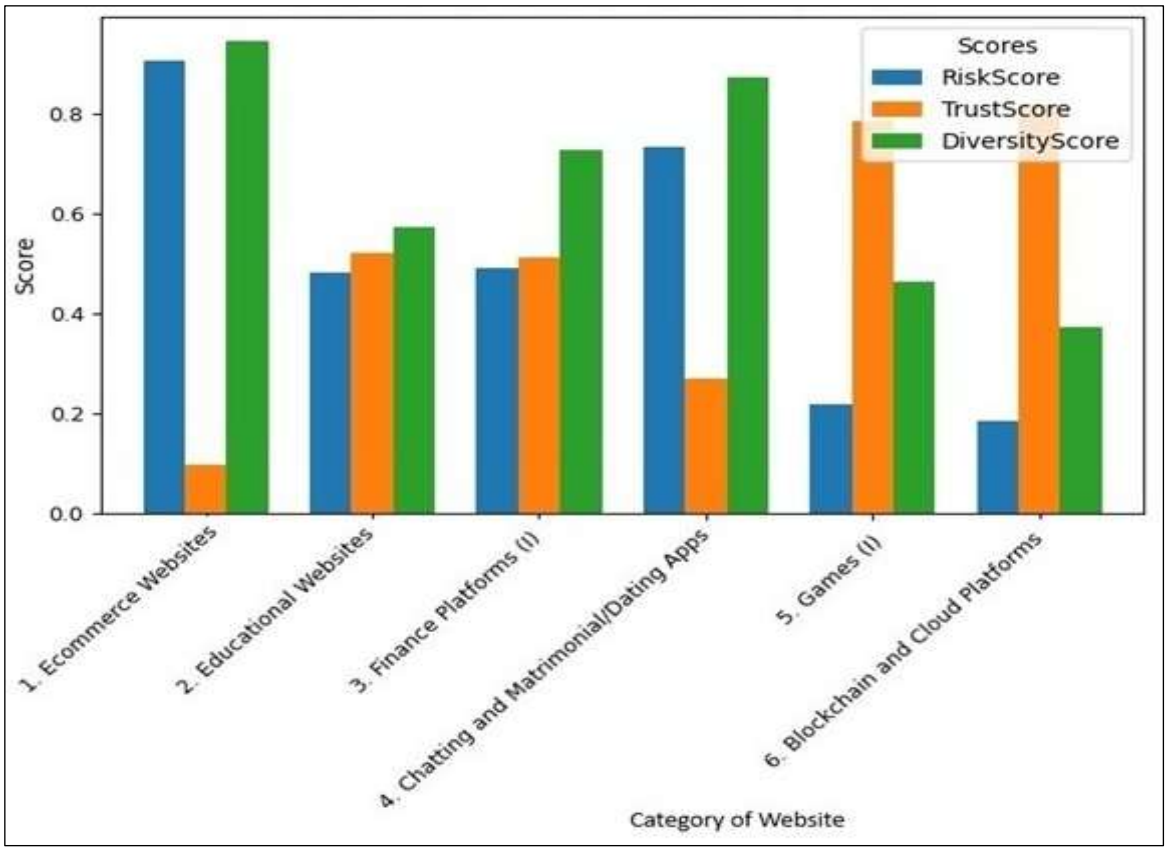

Figure 3:Category-wise Comparison Bar Chart.
Source: Authors, (2026).

The bar chart shows *RiskScore*, *TrustScore*, and *DiversityScore* for each category. In the heatmap, values are shown in matrix using color gradients instead of numbers. The heatmap highlights which scores are high/low with colors for quick comparison.

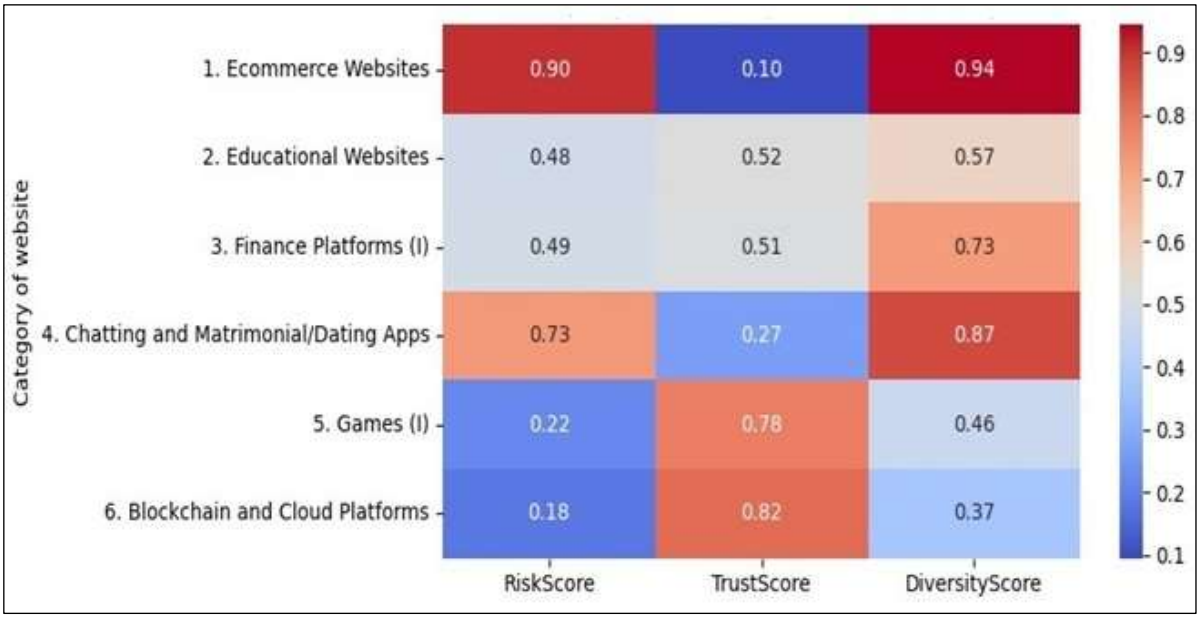

Figure 4: Category-wise Comparison Heatmap.
Source: Authors, (2026).

The charts in figure 3 and figure 4 reveal distinct sectoral differences in the prevalence and perception of dark patterns. E-commerce emerges as the highest-risk domain, characterized by the lowest levels of user trust and the widest variety of manipulative practices, reflecting how aggressive platforms optimize for sales. Dating apps also register as high risk with similarly low trust, as their designs often exploit emotional vulnerability and urgency. In contrast, finance and education platforms occupy a middle ground, showing moderate levels of risk, trust, and manipulation diversity due to stronger regulation in finance and ethical expectations in education. Interestingly, games and blockchain applications appear at the opposite end of the spectrum, with the lowest risk and highest trust, suggesting that users perceive these environments as more transparent or voluntary in nature, even though they operate in highly interactive and experimental domains. Overall, E-commerce and Dating Apps are the most manipulative, Finance and Education are moderately manipulative, while Games and Blockchain/Cloud Platforms are the least manipulative and most trusted.

V. CONCLUSIONS

To effectively mitigate dark patterns, a multi-stakeholder approach is essential. For designers and developers, the priority should be integrating ethical design toolkits and real-time pattern checkers into everyday workflows, alongside adopting standardized UI guidelines that reduce manipulative elements. Regulators and policymakers can play a crucial role by establishing regulatory sandboxes, where platforms can test interfaces for compliance, introducing legal UX audits or certification schemes modeled on GDPR and CCPA, and mandating enforceable design standards backed by penalties for non-compliance. Moreover, India's regulatory trajectory demonstrates a growing commitment to curbing digital exploitation, but sustained investment in technical expertise, consumer education, and coordinated enforcement is essential to ensure that these protections deliver on their promise. Users and communities should be empowered through digital literacy campaigns and gamified tools that enhance their ability to recognize manipulative interfaces, while participatory co-design with vulnerable groups, such as low-literacy, mobile-first, and multilingual population which ensure that regulations and design practices reflect diverse needs. Finally, researchers must shift focus from detection towards intervention, developing frameworks that can address dark patterns in emerging domains like extended reality, voice interfaces, and algorithmic platforms. Together, these strategies can move governance from reactive detection towards proactive prevention, fostering more transparent, equitable, and trustworthy digital environments.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Preeti Marwaha, Shalu Mahajan, Ishitva Joshi, Kriti Mishra, Ananya, Priyanka Sharma, Arunita Chaukiyal.
Methodology: Preeti Marwaha, Shalu Mahajan, Ishitva Joshi, Kriti Mishra, Ananya, Priyanka Sharma, Arunita Chaukiyal.
Investigation: Preeti Marwaha, Shalu Mahajan, Ishitva Joshi, Kriti Mishra, Ananya, Priyanka Sharma, Arunita Chaukiyal..
Discussion of results: Preeti Marwaha, Shalu Mahajan, Ishitva Joshi, Kriti Mishra, Ananya, Priyanka Sharma, Arunita Chaukiyal..
Writing – Original Draft: Preeti Marwaha, Shalu Mahajan, Ishitva Joshi, Kriti Mishra, Ananya, Priyanka Sharma, Arunita Chaukiyal.
Writing – Review and Editing: Preeti Marwaha, Shalu Mahajan, Ishitva Joshi, Kriti Mishra, Ananya, Priyanka Sharma, Arunita Chaukiyal.
Resources: Preeti Marwaha, Shalu Mahajan, Ishitva Joshi, Kriti Mishra, Ananya, Priyanka Sharma, Arunita Chaukiyal.
Supervision: Preeti Marwaha, Shalu Mahajan, Ishitva Joshi, Kriti Mishra, Ananya, Priyanka Sharma, Arunita Chaukiyal.
Approval of the final text: Preeti Marwaha, Shalu Mahajan, Ishitva Joshi, Kriti Mishra, Ananya, Priyanka Sharma, Arunita Chaukiyal.

VII. REFERENCES

[1] A. R. Casare, C. G. Da Silva, and R. Moraes, "User perception as a factor for improving trustworthiness in e-commerce systems," *Journal on Interactive Systems*, vol. 15, no. 1, pp. 194–219, 2024. doi: 10.5753/jis.2024.3748.

[2] J. Donia and J. A. Shaw, "Ethics and values in design: A structured review and theoretical critique," *Science and Engineering Ethics*, vol. 27, no. 5, p. 57, 2021.

[3] V. Bhaskaran, "Designing for trust: The crucial role in digital user experiences," *Journal of User Experience*, vol. 19, no. 2, pp. 53–59, 2024.

[4] L. Zhang-Kennedy, M. Keleher, and M. Valiquette, "Navigating the gray: Design practitioners' perceptions toward the implementation of privacy dark patterns," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. CSCW1, pp. 1–26, 2024. doi: 10.1145/3637374.

[5] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The dark (patterns) side of UX design," in *Proc. CHI Conf. Human Factors in Computing Systems*, 2018, pp. 1–14.

[6] S. S. Chivukula and C. M. Gray, "Co-evolving towards evil design outcomes: Mapping problem and solution process moves," in *Proc. DRS*, 2020. doi: 10.21606/drs.2020.107.

[7] N. G. Devarmani *et al.*, "The fake discount epidemic in e-commerce platform: An examination of tactics, tools, and consumer awareness," *Cuestiones de Fisioterapia*, vol. 54, no. 1, pp. 796–807, 2025. doi: 10.48047/va8ybt47.

[8] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence," in *Proc. CHI Conf. Human Factors in Computing Systems*, 2020, pp. 1–13.

[9] D. Kelly and V. L. Rubin, "Identifying dark patterns in user account disabling interfaces: Content analysis results," *Social Media + Society*, vol. 10, no. 1, 2024, Art. no. 20563051231224269.

[10] R. F. Muhammad and S. Kasahara, "Agent-based simulation of fake news dissemination: The role of trust assessment and big five personality traits on news spreading," *Social Network Analysis and Mining*, vol. 14, no. 1, p. 75, 2024.

[11] M. Botes, "Autonomy and the social dilemma of online manipulative behavior," *AI and Ethics*, vol. 3, no. 1, pp. 315–323, 2023.

[12] L. Alberts, U. Lyngs, and M. Van Kleek, "Computers as bad social actors: Dark patterns and anti-patterns in interfaces that act socially," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. CSCW1, pp. 1–25, 2024.

[13] A. Gerl and D. Pohl, "Critical analysis of LPL according to Articles 12–14 of the GDPR," in *Proc. 13th Int. Conf. Availability, Reliability and Security*, 2018, pp. 1–9. doi: 10.1145/3230833.3233267.

[14] Department of Consumer Affairs, *Draft Guidelines for Prevention and Regulation of Dark Patterns*. Ministry of Consumer Affairs, Government of India, 2023. [Online]. Available: https://consumeraffairs.nic.in

[15] J. Luguri and L. J. Strahilevitz, "Shining a light on dark patterns," *Journal of Legal Analysis*, vol. 13, no. 1, pp. 43–109, 2021. doi: 10.1093/jla/laz004.

[16] A. Mathur *et al.*, "Dark patterns at scale: Findings from a crawl of 11K shopping websites," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–32, 2019.

[17] A. Ramteke, S. Tembhurne, G. Sonawane, and R. N. Bhimanpallewar, "Detecting deceptive dark patterns in e-commerce platforms," *arXiv preprint* arXiv:2406.01608, 2024.

[18] J. Chen *et al.*, "Unveiling the tricks: Automated detection of dark patterns in mobile applications," in *Proc. 36th Annu. ACM Symp. User Interface Software and Technology*, 2023, pp. 1–20. doi: 10.1145/3586183.3606783.

[19] M. Hilton, "Dark patterns and user mental health: Identifying theoretical impacts of deceptive design on vulnerable demographics," in *Proc. Human Factors and Ergonomics Society Annu. Meeting*, vol. 67, no. 1, pp. 2124–2127, 2023.

[20] V. Krauß *et al.*, "What makes XR dark? Examining emerging dark patterns in augmented and virtual reality through expert co-design," *ACM Trans. Comput.-Hum. Interact.*, vol. 31, no. 3, pp. 1–39, 2024.

[21] J. Gunawan, A. Pradeep, D. Choffnes, W. Hartzog, and C. Wilson, "A comparative study of dark patterns across web and mobile modalities," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW2, pp. 1–29, 2021. doi: 10.1145/3479521.

[22] J. P. Zagal, S. Björk, and C. Lewis, "Dark patterns in the design of games," in *Foundations of Digital Games*, 2013.

[23] C. M. Gray, T. Mildner, and R. Gairola, "Getting trapped in Amazon's 'Iliad Flow': A foundation for the temporal analysis of dark patterns," in *Proc. CHI Conf. Human Factors in Computing Systems*, 2025, pp. 1–10. doi: 10.1145/3706598.3713828.

[24] D. Green, "Strategic indeterminacy and online privacy policies: (Un) informed consent and the General Data Protection Regulation," *International Journal for the Semiotics of Law*, vol. 38, no. 2, pp. 701–729, 2025.

[25] M. Degeling *et al.*, "We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy," *arXiv preprint* arXiv:1808.05096, 2018.

[26] J. Chen *et al.*, "From exploration to revelation: Detecting dark patterns in mobile apps," *arXiv preprint* arXiv:2411.18084, 2024.

[27] L. Nie *et al.*, "Shadows in the interface: A comprehensive study on dark patterns," *Proceedings of the ACM on Software Engineering*, vol. 1, no. FSE, p. 204–225, 2024. doi: 10.1145/364373.

[28] S. Santana, S. K. Dallas, and V. G. Morwitz, "Consumer reactions to drip pricing," *Marketing Science*, vol. 39, no. 1, pp. 188–210, 2020. doi: 10.1287/mksc.2019.1207.

[29] E. Moriuchi and S. Murdy, "Consumer reactions to drip pricing: The moderating effect of price fairness in the sharing economy accommodation," *Cornell Hospitality Quarterly*, vol. 66, no. 3, pp. 304–316, 2025. doi: 10.1177/19389655241271328.

[30] S. A. Goodstein, "When the cat's away: Techlash, loot boxes, and regulating 'dark patterns' in the video game industry's monetization strategies," *Univ. Colo. Law Rev.*, vol. 92, pp. 285–330, 2021.

[31] A. Singh, A. Arun, P. Malhotra, P. Desur, A. Jain, D. H. Chau, and P. Kumaraguru, "Erasing labor with labor: Dark patterns and lockstep behaviors on Google Play," in *Proc. 33rd ACM Conf. Hypertext and Social Media*, 2022, pp. 186–191. doi: 10.1145/3511095.3536368.

[32] B. Schaffner, N. A. Lingareddy, and M. Chetty, "Understanding account deletion and relevant dark patterns on social media," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW2, pp. 1–43, 2022.

[33] J. Aagaard, M. E. C. Knudsen, P. Bækgaard, and K. Doherty, "A game of dark patterns: Designing healthy, highly-engaging mobile games," in *Proc. CHI Conf. Human Factors in Computing Systems Extended Abstracts*, 2022, pp. 1–8.

[34] E. Dula, A. Rosero, and E. Phillips, "Identifying dark patterns in social robot behavior," in *Proc. 2023 Systems and Information Engineering Design Symp. (SIEDS)*, 2023, pp. 7–12.

[35] I. Stavrakakis, A. Curley, D. O'Sullivan, D. Gordon, and B. Tierney, "A framework of web-based dark patterns that can be detected manually or automatically," 2021.

[36] Y. Lu, C. Zhang, Y. Yang, Y. Yao, and T. J. Li, "From awareness to action: Exploring end-user empowerment interventions for dark patterns in UX," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. CSCW1, pp. 1–41, 2024. doi: 10.1145/3637336.

[37] W. Yi and Z. Li, "Mapping the scholarship of dark pattern regulation: A systematic review of concepts, regulatory paradigms, and solutions from an interdisciplinary perspective," *arXiv preprint* arXiv:2407.10340, 2024. doi: 10.48550/arXiv.2407.10340.

[38] V. Singh, N. K. Vishvakarma, H. Mal, and V. Kumar, "Prioritizing dark patterns in the e-commerce industry—an empirical investigation using analytic hierarchy process," *Measuring Business Excellence*, vol. 28, no. 2, pp. 177–192, 2024. doi: 10.1108/MBE-08-2023-0114.

[39] R. Chaudhary, S. Jain, R. Gupta, and V. Aggarwal, "Understanding the psychology of impulse buying in e-commerce: A behavioral review," *Journal of Marketing & Social Research*, vol. 2, pp. 102–113, 2025. doi: 10.61336/jmsr/25-06-13.

[40] C. Santos, N. Bielova, and C. Matte, "Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners," *arXiv preprint* arXiv:1912.07144, 2019.

[41] B. M. Berens *et al.*, "Cookie disclaimers: Dark patterns and lack of transparency," *Computers & Security*, vol. 136, p. 103507, 2024. doi: 10.1016/j.cose.2023.103507.

[42] V. Singh, N. K. Vishvakarma, and V. Kumar, "Profit over principles: unveiling the motivating factors behind dark patterns in e-commerce through the lens of agency theory," *Journal of Enterprise Information Management*, vol. 38, no. 3, pp. 821–848, 2025.

[43] S. Santana, S. K. Dallas, and V. G. Morwitz, "Consumer reactions to drip pricing," *Marketing Science*, vol. 39, no. 1, pp. 188–210, 2020. doi: 10.1287/mksc.2019.1207.

[44] A. Fecher, T. Robbert, and S. Roth, "Same price, different perception: Measurement-unit effects on price-level perceptions and purchase intentions," *Journal of Retailing and Consumer Services*, vol. 49, pp. 129–142, 2019.

[45] G. Ahmetoglu, A. Furnham, and P. Fagan, "Pricing practices: A critical review of their effects on consumer perceptions and behaviour," *Journal of Retailing and Consumer Services*, vol. 21, no. 5, pp. 696–707, 2014. doi: 10.1016/j.jretconser.2014.04.013.

[46] K. M. Ramokapane, A. C. Mazeli, and A. Rashid, "Skip, skip, skip, accept!!!: A study on the usability of smartphone manufacturer provided default features and user privacy," *arXiv preprint* arXiv:2308.14593, 2023.

[47] F. Nguyen, "Trial length, pricing, and rationally inattentive customers," *arXiv preprint* arXiv:2507.06422, 2025.

[48] X. Ye, "Dark patterns and addictive designs," *Weizenbaum Journal of the Digital Society*, vol. 5, no. 3, 2025.

[49] K. Oyibo, "The influence of user knowledge and usage behaviour on decision-making and perceived reputation of streaming sites that use dark patterns," *Behaviour & Information Technology*, pp. 1–20, 2025. doi: 10.1080/0144929X.2024.2447475.

[50] F. Nygren and P. Tran, "Streaming in the dark: Analysing video streaming services for dark patterns: A user interface study," 2024.

[51] D. M. Rhomberg, "Dark patterns for good? Exploring end-user perspectives on bright patterns to counteract perceived social media problems," Ph.D. dissertation, Technische Universität Wien, 2024. doi: 10.34726/hss.2024.114637.

[52] E. Alashwali *et al.*, "Interface design to support informed choices when users face numerous privacy decisions," *IEEE Trans. Privacy*, 2025.

[53] M. Mattiuzzo and P. P. Ponce, "Power through design—dark patterns, personalization and the emergence of TikTok," *Int. Rev. Law, Comput. & Technol.*, vol. 39, no. 1, pp. 30–54, 2025. doi: 10.1080/13600869.2024.2351672.

[54] M. Dubiel, A. Sergeeva, and L. A. Leiva, "Impact of voice fidelity on decision making: A potential dark pattern?," in *Proc. 29th Int. Conf. Intelligent User Interfaces*, 2024, pp. 181–194. doi: 10.1145/3640543.3645202.

[55] D. Franzen, C. Müller-Birn, and O. Wegwarth, "Communicating the privacy-utility trade-off: Supporting informed data donation with privacy decision interfaces for differential privacy," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. CSCW1, pp. 1–56, 2024.

[56] M. Beltrán, "Defining, classifying and identifying addictive patterns in digital products," *IEEE Trans. Technol. & Soc.*, 2025.

[57] L. Clark and M. Zack, "Engineered highs: Reward variability and frequency as potential prerequisites of behavioural addiction," *Addictive Behaviors*, vol. 140, p. 107626, 2023.

[58] Q. Mamun, "Technology and social media's hidden cost: Social dilemma, mental health, misinformation, and manipulative practices," 2025.

[59] S. Ahuja and J. Kumar, "Conceptualizations of user autonomy within the normative evaluation of dark patterns," *Ethics and Information Technology*, vol. 24, no. 4, p. 52, 2022.

[60] G. Freeman, K. Wu, N. Nower, and D. Y. Wohn, "Pay to win or pay to cheat: How players of competitive online games perceive fairness of in-game purchases," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CHI PLAY, pp. 1–24, 2022. doi: 10.1145/3549510.

[61] C. J. Larche, K. Chini, C. Lee, M. J. Dixon, and M. Fernandes, "Rare loot box rewards trigger larger arousal and reward responses, and greater urge to open more loot boxes," *Journal of Gambling Studies*, vol. 37, no. 1, pp. 141–163, 2021.

[62] L. Wang *et al.*, "Reduced loss aversion and inhibitory control in adolescents with internet gaming disorder," *Psychology of Addictive Behaviors*, vol. 34, no. 3, pp. 484–494, 2020. doi: 10.1037/adb0000549.

[63] S. Raiha *et al.*, "Altered reward processing system in internet gaming disorder," *Frontiers in Psychiatry*, vol. 11, p. 599141, 2020. doi: 10.3389/fpsyt.2020.599141.

[64] W.-R. Zhou *et al.*, "Imbalanced sensitivities to primary and secondary rewards in internet gaming disorder," *Journal of Behavioral Addictions*, vol. 10, no. 4, pp. 990–1004, 2021. doi: 10.1556/2006.2021.00072.

[65] J. Frommel and R. L. Mandryk, "Daily quests or daily pests? The benefits and pitfalls of engagement rewards in games," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CHI PLAY, pp. 1–23, 2022. doi: 10.1145/3549489.

[66] J. Salminen, M. Mustak, S.-G. Jung, H. Makkonen, and B. J. Jansen, "Decoding deception in the online marketplace: Enhancing fake review detection with psycholinguistics and transformer models," *Journal of Marketing Analytics*, 2025.

[67] Y. Sazid and K. Sakib, "Prevalence and user perception of dark patterns: A case study on e-commerce websites of Bangladesh," in *Proc. ENASE*, 2024, pp. 238–249.

[68] P. S. Kodmurgi *et al.*, "ScrapeAI: A multi-modal approach to detect dark patterns," in *Proc. 15th Int. Conf. Computing Communication and Networking Technologies (ICCCNT)*, 2024, pp. 1–6. doi: 10.1109/ICCCNT61001.2024.10723319.

[69] S. M. H. Mansur, S. Salma, D. Awofisayo, and K. Moran, "Aidui: Toward automated recognition of dark patterns in user interfaces," in *Proc. IEEE/ACM 45th Int. Conf. Software Engineering (ICSE)*, 2023, pp. 1958–1970.

[70] A. Bajaj, K. Uppal, R. Razdan, Y. Tuteja, A. Bhardwaj, and A. Abraham, "A comprehensive analysis for dark pattern detection using structural, visual and textual information," *Int. J. Comput. Inf. Syst. Ind. Manage. Appl.*, vol. 17, p. 12, 2025. doi: 10.70917/ijcisim-2025-0002.

[71] R. Vedhapriyavadhana, P. Bharti, and S. Chidambaranathan, "Detecting dark patterns in shopping websites—A multi-faceted approach using BERT," *Enterprise Information Systems*, 2025, Art. no. 2457961.

[72] P. Hausner and M. Gertz, "Dark patterns in the interaction with cookie banners," *arXiv preprint* arXiv:2103.14956, 2021.

[73] R. Schäfer *et al.*, "Fighting malicious designs: Towards visual countermeasures against dark patterns," in *Proc. CHI Conf. Human Factors in Computing Systems*, 2024, pp. 1–13.

[74] K. Kronhardt, K. Rolfes, and J. Gerken, "Trickery: Exploring a serious game approach to raise awareness of deceptive patterns," in *Proc. Int. Conf. Mobile and Ubiquitous Multimedia*, 2024, pp. 133–147.

[75] A. Rana, "UX audit: A comprehensive review of methodologies and best practices for evaluating user experiences," *Int. J. Arts Archit. & Design*, vol. 2, no. 1, pp. 53–54, 2024.

[76] Norwegian Consumer Council, *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, 2018.

[77] M. Ghosh and K. Sarma, "Understanding consumer rights and responsibilities through consumer protection act 2019," *Int. J. Manage.*, vol. 11, no. 11, 2020.

[78] N. Gupta and A. George, "Digital personal data protection act, 2023: Charting the future of India's data regulation," in *Data Governance and the Digital Economy in Asia*, Routledge, 2025, pp. 34–53.

[79] S. Guha and S. Matilal, "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021—A reassessment of the contours and limits," *NUJS J. Regul. Stud.*, vol. 8, p. 32, 2023.

[80] M. Guruswamy, "Justice K. S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors.," *Am. J. Int. Law*, vol. 111, no. 4, pp. 994–1000, 2017.

[81] A. Narayanan, A. Mathur, M. Chetty, and M. Kshirsagar, "Dark patterns: Past, present, and future: The evolution of tricky user interfaces," *Queue*, vol. 18, no. 2, pp. 67–92, 2020.

[82] X. Zhan, Y. Xu, N. Abdi, J. Collenette, R. Abu-Salma, and S. Sarkadi, "Banal deception human-AI ecosystems: A study of people's perceptions of LLM-generated deceptive behaviour," *arXiv preprint* arXiv:2406.08386, 2024. doi: 10.48550/arXiv.2406.08386.

[83] R. P. Dahlan and M. Susanty, "Finding dark patterns in casual mobile games using heuristic evaluation," 2022. doi: 10.33322/petir.v15i2.1151.

[84] M. G. de Matos and I. Adjerid, "Consumer consent and firm targeting after GDPR: The case of a large telecom provider," *Management Science*, vol. 68, no. 5, pp. 3330–3378, 2022. doi: 10.1287/mnsc.2021.4054.

[85] C. F. Mondschein, "Some iconoclastic thoughts on the effectiveness of simplified notices and icons for informing individuals as proposed in Article 12 (1) and (7) GDPR," *Eur. Data Prot. L. Rev.*, vol. 2, p. 507, 2016.

[86] I. Gupta and P. Naithani, "Transparent communication under Article 12 of the GDPR: Advocating a standardised approach for universal understandability," *Journal of Data Protection & Privacy*, vol. 5, no. 2, pp. 149–161, 2022.

[87] J. Yao and H. Wei, “Creating better-informed consumers and reducing dark pattern tendencies through improved terms of service solutions,” 2018.

[88] V. Singh, N. K. Vishvakarma, and V. Kumar, “Investigating consumer challenges against dark patterns using grey influence analysis (GINA),” *Marketing Intelligence & Planning*, 2025. doi: 10.1108/mip-08-2024-0538.

[89] V. Singh, N. K. Vishvakarma, and V. Kumar, “Dark patterns, dimmed brands: The erosion of equity through deceptive design in e-commerce,” *Internet Research*, 2025. doi: 10.1108/intr-07-2024-1026.

[90] A. Zac, Y.-C. Huang, A. von Moltke, C. Decker, and A. Ezrachi, “Dark patterns and consumer vulnerability,” *Behavioural Public Policy*, pp. 1–50, 2023. doi: 10.1017/bpp.2024.49.

[91] A. M. Bhoot, M. A. Shinde, and W. P. Mishra, “Towards the identification of dark patterns: An analysis based on end-user reactions,” in *Proc. 11th Indian Conf. Human-Computer Interaction*, 2020, pp. 24–33. doi: 10.1145/3429290.3429293.

[92] W. C. Koh and Y. Z. Seah, “Unintended consumption: The effects of four e-commerce dark patterns,” *Cleaner and Responsible Consumption*, vol. 11, p. 100145, 2023. doi: 10.1016/j.clrc.2023.100145.

[93] Q. Li, Y. Liu, and C. Chen, “Satisfaction and continuation intention in music streaming services: Investigating key factors for user retention,” *Frontiers in Psychology*, vol. 16, p. 1552800, 2025.

[94] A. Hung, “Keeping consumers in the dark: Addressing ‘nagging’ concerns and injury,” *Colum. L. Rev.*, vol. 121, pp. 2483–2525, 2021.

[95] D. Li, “The FTC and the CPRA’s regulation of dark patterns in cookie consent notices,” *Univ. Chicago Business Law Rev.*, vol. 1, no. 1, pp. 19–42, 2022.

[96] R. W. Saaty, “The analytic hierarchy process—what it is and how it is used,” *Mathematical Modelling*, vol. 9, no. 3–5, pp. 161–176, 1987. doi: 10.1016/0270-0255(87)90473-8.

[97] C. E. Shannon, “A mathematical theory of communication,” *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 1, pp. 3–55, 2001. doi: 10.1145/584091.584093.