

Rethinking Interface Design in the Digital Society: Dark Patterns and Governance Strategies

Ning Li, Tuliguri

Institute for History of Science and Technology, Inner Mongolia Normal University, Hohhot, China
Email: ln778339748@163.com

How to cite this paper: Li, N. and Tuliguri (2025) Rethinking Interface Design in the Digital Society: Dark Patterns and Governance Strategies. *Journal of Computer and Communications*, 13, 83-98.
<https://doi.org/10.4236/jcc.2025.1311007>

Received: November 11, 2025

Accepted: November 18, 2025

Published: November 21, 2025

Copyright © 2025 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

With the widespread application of digital platforms, interface design has evolved from mere information presentation into a crucial tool for shaping user behavior. As a design strategy that covertly manipulates user choices through visual, linguistic, and interactional pathways, dark patterns have been extensively embedded in sectors such as e-commerce, finance, education, healthcare, and social networking. Supported by big data analytics, algorithmic prediction, and behavioral modeling, dark patterns exploit users' cognitive limitations and psychological biases to construct decision-making environments that appear free but are in fact controlled. This design practice has led to a series of social problems, including the infringement of user interests, cognitive manipulation, and privacy leakage. Addressing these challenges requires the advancement of social governance of dark patterns through legal, ethical, and technical approaches in a coordinated manner.

Keywords

Digital Platforms, Interface Design, Dark Patterns, Governance

1. Introduction

As human society enters the digital era, interface design has increasingly become a crucial "bridge" connecting users and digital platforms. Interface design refers to the overall strategy of organizing, guiding, and regulating user behavior during human-computer interaction through visual elements, language expression, structural layout, and operational processes. It not only serves the function of presenting information, but also implicitly carries certain value orientations and interest-driven intentions [1]. Dark pattern design is a particular type of interface

design that covertly influences user choices through visual cues, linguistic framing, interaction pathways, and structural arrangements. This design approach has now been widely embedded across commercial platforms, governmental services, educational applications, and other digital environments, triggering extensive discussions about user rights, cognitive intervention, and the impact on decision-making autonomy.

Current research on Dark Patterns has mainly focused on their impacts, typologies, and application fields. For example, Thaler and Sunstein (2008) pointed out the strong influence of Dark Patterns on users' decision-making [2]. Mathur *et al.* (2019) further revealed from legal and ethical perspectives that such design practices infringe upon users' autonomy [3]. Gray *et al.* (2018) identified and categorized common types of Dark Patterns in UX design [4]. Li Qian (2022), taking social media and live-streaming platforms as examples, demonstrated how interface strategies such as "path manipulation" and "visual misdirection" weaken users' fundamental rights in actual use [5]. Yang Fei (2023), through empirical research on e-commerce platforms, found that shopping apps commonly employ default opt-ins and hidden cancellation paths, thereby harming consumer autonomy [6]. Liu Ying (2023), based on a systematic review of Dark Pattern types and mechanisms, proposed corresponding legal governance measures [7].

Methodologically, this paper employs an interdisciplinary literature review and comparative analysis across HCI, legal studies, and ethics to examine the socio-technical mechanisms of dark pattern design.

2. Dark Patterns: Concept, Characteristics, and Classification

2.1. Concept of Dark Patterns

Interface design has undergone a gradual evolution from function-oriented to experience-oriented approaches, and further toward algorithm-driven and behavior-guiding models. Early Human-Computer Interaction (HCI) design emphasized improving operational efficiency, focusing on clear information architecture and intuitive operation. With the advent of the Web 2.0 era, interface design shifted toward prioritizing user experience and emotional interaction, gradually developing diverse design strategies such as visual guidance, process-oriented interaction, and personalized adaptation. In recent years, driven by data-centered design and context-aware computing, the interface has come to be regarded not only as a technical presentation layer, but also as a medium for behavioral guidance, emotional modulation, and commercial conversion.

Dark Patterns are a particular type of interface design formed under algorithmic decision-making and behavior-guidance mechanisms. Their purpose is to influence user choices through default options, visual cues, nested interaction pathways, and structural arrangements. The term Dark Patterns was first introduced by user experience designer Harry Brignull in 2010 to describe interface designs that deliberately mislead users into making decisions that benefit the platform

while being detrimental to their own interests, often under conditions of incomplete awareness or limited understanding [8]. It is precisely due to this characteristic of “appearing neutral while subtly guiding” that Dark Patterns have increasingly become a highly controversial interface design strategy within digital platforms [8].

In contrast, “persuasive design” or “nudging” techniques aim to guide users toward beneficial behaviors while preserving freedom of choice. Dark patterns, by contrast, prioritize platform interests through deception and constraint, thus representing an ethically problematic form of manipulation.

2.2. Characteristics of Dark Patterns

As a “mediating layer” in human-computer interaction, Dark Patterns exhibit several key characteristics, including technical dominance, inducement, control, and concealment.

First, technical dominance. Designers of Dark Patterns hold overwhelming advantages in interface construction and interaction, user data collection and utilization, algorithmic interpretation, and continuous optimization, which constitutes a form of technological monopoly that allows platforms to guide, induce, or even manipulate users covertly [9]. As Brignull notes, the essence of Dark Patterns lies in leveraging users’ cognitive blind spots, habitual operations, and contextual dependencies to construct an asymmetric choice environment, so that users complete platform-preferred actions under an illusion of freedom [8].

Second, inducement. Dark Patterns often deploy visual or psychological strategies—such as highlighting recommended options, encouraging language, loss-framed prompts, countdown timers, and scarcity emphasis—to steer users toward platform-benefiting behaviors in moments of reduced deliberation; for instance, e-commerce promotions frequently present prompts like “only a few items left” or “most users have already purchased” to manufacture urgency and scarcity, thereby accelerating decisions [3].

Third, control. Although users appear to retain freedom of choice, their decisions are effectively made within a restricted and manipulated cognitive environment; this systematic shaping and guidance of behavior amount to a subtle yet highly efficient form of technological domination [7]. In practice, attempts to cancel subscriptions, log out, or disable features often encounter multi-layered menus and repeated confirmations; for example, video platforms commonly pre-select automatic renewal, while disabling it requires navigating several hidden interface layers [6].

Finally, concealment. Dark Patterns operate as a kind of covert discipline: through ambiguous terminology, procedural complexity, hidden pathways, and visual prioritization, platforms present an appearance of “free choice” while steering users away from fully rational decisions; for example, key fee items in loan application flows may be buried under “expand more” menus or visually downplayed to reduce salience [4].

2.3. Classification of Dark Patterns

Different types and intensities of Dark Patterns vary across interface environments [10]. Based on their influencing mechanisms and degrees of manipulation, Dark Patterns can generally be divided into inductive, deceptive, and coercive types [7].

First, inductive Dark Patterns do not directly restrict user choices, but instead guide users toward platform-preferred outcomes by setting default options, highlighting recommended items, or diminishing the visibility of alternative choices. The core mechanism here is the default effect, meaning that when a particular option is pre-selected, users are more likely to accept it rather than actively modify it [2]. This tendency becomes especially pronounced in situations involving high cognitive load or decision uncertainty.

Second, deceptive Dark Patterns mislead users by means of information concealment, lengthy text, vague terminology, and linguistic framing, causing them to make platform-favorable decisions without fully understanding the implications. This type of manipulation primarily exploits cognitive biases and information asymmetry. For example, in a study of 26 Norwegian financial applications, Raković and Inal found disguised pricing structures, hidden fees, and complex cancellation pathways to be widespread—particularly in non-bank financial products [11].

Third, coercive Dark Patterns influence user decision-making through forced procedural steps, time pressure, and emotional manipulation, thereby eroding users' substantive freedom of choice. The core mechanisms involved include loss aversion, time urgency, and psychological pressure. For instance, in some subscription services, users attempting to cancel are required to navigate multi-layered menus or complete lengthy confirmation procedures, and may even be forced to call customer service or fill out detailed surveys, significantly increasing the difficulty and psychological burden of cancellation. This structure resembles a form of soft coercion [12].

In practice, however, many platforms use these forms in combination: beginning with inductive design to lower user vigilance, followed by deceptive wording to obscure key information, and finally applying coercive mechanisms to ensure alignment with platform-preferred outcomes. This progressive architecture of influence has become a core behavioral control strategy in contemporary digital platform environments.

3. Main Strategies, Technical Support, and Cognitive Background of Dark Pattern Design

3.1. Main Strategies of Dark Pattern Design

The effectiveness of Dark Patterns in influencing user decisions lies in their strategic use of multiple design techniques during the interface structuring and interaction process, including default settings, textual terminology, path guidance, and structural arrangement.

First, default settings. Digital platforms frequently set options favorable to data collection, additional features, or subscription renewals as the default state. If users do not actively change these settings, consent is assumed. In practice, users tend to maintain default configurations rather than expend cognitive effort to locate and modify them—this phenomenon is known as the “default effect” [6]. Due to users’ limited understanding of data usage consequences, they often remain unaware of the behavioral costs or privacy risks embedded within default options.

Second, textual terminology. In privacy policies, data authorization statements, and responsibility clauses, platforms often employ ambiguous wording and lengthy descriptions, which obscure the actual meaning and consequences of user selections. As Miranda Fricker notes, professionalized language can effectively exclude many users from meaningful cognitive participation, preventing them from fully understanding their situational context [13]. Even when users complete the required actions of “reading” and “agreeing,” they may still not comprehend the real implications of their decisions.

Third, path guidance. Beyond linguistic framing, digital platforms rely heavily on non-verbal interface elements—such as color contrast, button size, visual focus, and information hierarchy—to direct users’ attention and behavioral patterns. These subtle guidance mechanisms increase the likelihood of users selecting platform-preferred options, while ignoring alternatives that may better protect their interests. Gray *et al.* argue that the essence of such “cognitive disciplining” lies in which information is made most visible [4]. By following visually suggested routes, users often complete intended operations without reflection.

Finally, structural design. Platforms strategically manipulate interface structure so that options beneficial to users become inconvenient, hidden, or difficult to access, while options advantageous to the platform are made convenient, salient, and easily accessible. For instance, cancellation pathways may be buried under multiple menu layers, while account logout may be intentionally complicated [12]. Moreover, Dark Pattern design often forms a “trigger–feedback–dependency” loop, cultivating behavioral habits that invisibly guide and reinforce user choices [14].

3.2. Technical Support of Dark Pattern Design

Dark Pattern design is not an incidental interface flaw, but a deliberately engineered apparatus—a comprehensive technological manipulation system jointly driven by big data, algorithmic inference, behavioral science, and interface aesthetics.

First, Dark Pattern design is grounded in the deep extraction of user information. Platforms do not merely collect users’ basic identity information and browsing behaviors; they also analyze fine-grained behavioral traces such as click pathways, time spent on specific elements, and preference signals. These micro-behavioral indicators are used to construct accurate user profiles and predictive behavior models. Through continuous updates enabled by deep learning methods,

platforms are capable of inferring user intentions with increasing precision, thereby formulating customized interface manipulation strategies. For example, a platform may analyze a user's response latency and frequency when interacting with "exit" or "decline" buttons in past interfaces, infer the user's psychological threshold or hesitation pattern, and accordingly adjust the intensity of persuasive prompts or the visibility of exit pathways.

Second, Dark Pattern design relies on meticulously structured interfaces as the operational medium. Interface design typically includes information architecture, visual guidance, linguistic and symbolic cues, and interaction feedback. Under ordinary circumstances, these techniques help reduce cognitive load and improve user experience. However, in Dark Pattern design, these elements are strategically repurposed as tools of control. In information architecture, platforms may increase the number of layers required to cancel a service; in visual presentation, acceptance options are highlighted using strong color contrast while rejection options are visually minimized; in linguistic expression, ambiguous or euphemistic phrasing is used to conceal material consequences; and in interaction feedback, friction and psychological pressure are deliberately crafted to prevent user actions that may disadvantage the platform [15]. As scholars have noted, Dark Patterns in privacy interfaces are not isolated design accidents, but represent a systematized mechanism of interface manipulation [3].

Third, Dark Pattern design is fundamentally enabled by multiple algorithmic techniques. The functioning of the interface depends on user profiling, algorithmic prediction, and behavioral modeling. User profiling enables platforms to identify preference structures and habitual tendencies, which directly inform default-setting strategies, pop-up timing, and interface prompts. Algorithmic prediction is used to detect the moments when users are most susceptible to influence, allowing platforms to precisely deliver "exclusive offers," "time-limited deals," or "scarcity messages." Meanwhile, behavioral models, drawing on psychology and behavioral economics, embed cognitive principles such as loss aversion, time pressure, and confirmation bias into interface interactions, thereby shaping user decision-making processes [16].

3.3. Cognitive Background of Dark Pattern Design

The effective functioning of Dark Patterns relies on a deep understanding of human cognitive patterns and psychological mechanisms, enabling users to perform platform-preferred actions while believing they are acting autonomously.

First, dark pattern design exploits users' knowledge limitations. There is a significant cognitive gap between technology designers and ordinary users in terms of algorithmic literacy, interface logic, and terminology comprehension. Most users lack the ability to recognize the design intentions and potential risks embedded in interface language, making it difficult for them to accurately evaluate what they are being guided to do [17]. Research by Eslami and colleagues shows that users are often unaware of the presence of algorithms and misinterpret recommenda-

tion results based on everyday assumptions rather than actual computational mechanisms [18].

Second, dark pattern design takes advantage of informational asymmetry. Interfaces frequently employ information masking strategies—technical jargon, obscure phrasing, lengthy clauses, and complex procedures—so that information is formally disclosed but substantively incomprehensible, producing a condition of “apparent transparency but practical opacity” [19]. Under limited rationality and decision fatigue, individuals tend to rely on heuristics, which allows platforms to influence decisions by manipulating default options, persuasive wording, and visual emphasis [2].

Third, dark pattern design exploits users’ psychological limitations. Users are not always rational decision-makers. Platforms deliberately create a sense of urgency, scarcity, or social conformity, prompting immediate emotional responses instead of reflective judgment. Recent behavioral economics and HCI research has shown that dark pattern strategies are frequently built upon psychological mechanisms such as the default effect, visual attention bias, and loss aversion [7] [20]. For instance, during account registration on social media or e-commerce applications, users are often required to agree to privacy policies before proceeding. These documents are typically long, technical, and filled with ambiguous legal terminology, making it difficult for users to fully understand the implications and risks in a short period of time.

4. The Application of Dark Patterns and Their Social Implications

Issues related to dark pattern design are not limited to economic sectors such as e-commerce and finance; they also occur widely in healthcare, education, legal services, recruitment, and other social domains. According to the 2024 annual investigation report released by the Global Privacy Enforcement Network (GPEN), the majority of mainstream websites and applications worldwide employ at least one form of dark pattern in their data collection interfaces, with common strategies including pre-checked consent boxes, complex terminology surrounding sensitive options, and weakened or hidden “reject” buttons [21].

4.1. Dark Patterns in Economic Domains and Their Impacts

In e-commerce platforms, dark patterns are commonly embedded in key processes such as product recommendation, payment checkout, and after-sales service. Their primary function is to increase purchase conversions and maximize platform revenue. For example, checkout pages often pre-select options such as automatic renewal or bundled add-on purchases, causing users to incur additional charges if they fail to manually deselect them. Furthermore, platforms frequently display time-limited or scarcity-based prompts to induce quick, emotionally driven decisions.

In cancellation or refund processes, users are often required to navigate multi-

ple interface layers, repeated confirmation steps, or even customer service communication—creating path obstacles that discourage or prevent withdrawal. A well-known case is Amazon Prime, where cancellation requires navigating multiple redundant pages and repeated confirmation steps, representing a typical path-obstruction dark pattern [22]. According to the 2023 report of the European Insurance and Occupational Pensions Authority (EIOPA), such interface designs significantly increase the uptake of additional insurance products but simultaneously compromise user rights and information transparency, thus constituting clear instances of dark pattern manipulation [23].

4.2. Dark Pattern Design in Public Service Domains and Its Impacts

As dark pattern design extends from commercial platforms to public service sectors, it increasingly shapes user decisions in ways that favor institutional interests.

In the healthcare sector, dark patterns are often embedded in processes such as patient data authorization, informed consent, and subscription to medical services. Studies have shown that many digital health platforms—for example, telemedicine applications and chronic disease management systems—pre-select the option “data used for research purposes” during initial registration, while burying the cancellation path behind multiple layers of settings [24]. Meanwhile, clinical trial recruitment platforms frequently employ ambiguous terminology and fragmented disclosure, placing key risk-related information in non-prominent interface positions. For example, some targeted cancer therapy trial interfaces use phrases like “data will be used to improve future health outcomes” instead of explicitly stating that such data may be sold for commercial purposes, thereby framing consent in a more ethically appealing manner. Such practices pose significant challenges to the ethical foundations of public healthcare [25].

In the education sector, dark patterns are quietly influencing how individuals access knowledge and educational services. Online learning platforms in particular routinely employ strategies such as “default subscription,” “automatic course renewal,” and emotionally suggestive prompts to retain users. Research indicates that platforms such as Coursera and Udemy often pre-select automatic renewal and periodic notification functions at the time of registration, while the paths to disable these features are hidden within multiple layers of settings. During the cancellation process, users are frequently confronted with prompts such as “You may miss valuable learning opportunities” or “Your skill improvement window is closing,” leveraging the psychology of loss aversion to reinforce platform control [26].

4.3. Dark Pattern Design in Other Social Service Domains and Its Impacts

In legal consultation and job recruitment services, dark pattern design is often reflected in the complexification of contractual texts. Long passages of professional terminology and ambiguous expressions are frequently used to obscure key

clauses, leading users to accept additional fees or restrictive conditions without fully understanding their implications. For example, payment obligations, liability statements, and risk clauses are often embedded deep within lengthy agreements, prompting users to click “agree” out of convenience while overlooking potential legal consequences. As King and Stephan note, such interface strategies appear to uphold the principle of informed consent, yet rely on “structural legitimacy” in interface design to circumvent substantive disclosure obligations, thereby maximizing the platform’s interests [27].

In social and dating applications, dark pattern design is more closely associated with the manipulation of attention and emotional engagement. Social platforms curate the rhythm of interactions to encourage continuous participation, response, and feedback, fostering a sense of dependency on the platform. In their analysis of platforms such as Facebook, Instagram, and Tinder, Gray and colleagues highlight the widespread use of “interface hooks”—design elements that intentionally guide user attention and behavior to extend engagement time and increase data production [4]. For example, some popular dating apps hide the “unmatch” or “remove connection” buttons within multiple layers of menus, or display prompts such as “Are you sure you want to give up a potential connection?” before allowing disconnection, using emotional framing to reinforce user retention. Likewise, in privacy settings, options such as “display profile to strangers” or “sync contact list” are frequently pre-selected by default. If users do not actively opt out, they may unintentionally disclose personal information [28].

5. Constructing a Comprehensive Governance Framework for Dark Pattern Design

The core objective of dark pattern design is to maximize profit, user retention, and data extraction through interface manipulation. This approach has already gone beyond the traditional notion of “user experience optimization” and has evolved into a mechanism of interface control [29]. The embedded interests incentives, power asymmetry, and responsibility deflection within dark pattern design have thus become key issues in the governance of digital societies. Gunawan and colleagues refer to dark pattern practices as “disloyal design”, arguing that such platform behaviors should be regulated under frameworks related to unfair competition and consumer rights protection [30].

5.1. Legal Measures

As dark patterns become increasingly prevalent, regulatory and legislative bodies around the world have begun to address the impacts of such practices on user privacy, data security, and consumer rights. The European Union’s General Data Protection Regulation (GDPR) established one of the world’s most stringent data protection systems, requiring platforms to provide transparent consent processes and prohibiting the collection of user data through implicit consent or pre-selected options. The regulation further stipulates that users must be clearly informed of the meaning and consequences of their choices, and must retain the

right to withdraw consent [31]. In contrast, privacy protection in the United States is more decentralized, relying on state-level legislation and sector-based norms. Among them, the California Consumer Privacy Act (CCPA) stands out as a representative regulatory framework, requiring companies to disclose data usage practices more transparently and granting consumers the right to request data deletion [32].

In China, digital platform governance has increasingly shifted from traditional cybersecurity regulation toward broader concerns regarding interface fairness and user autonomy. The 2021 Regulations on the Administration of Algorithmic Recommendations for Internet Information Services explicitly prohibit platforms from using algorithms to induce addiction, manipulate behavior, or violate public order, and ensure that users must retain the right to disable personalized recommendations [33]. Although this regulation does not directly use the term “dark patterns,” it introduces preliminary constraints on interface-based behavioral manipulation. Meanwhile, the Personal Information Protection Law, Consumer Rights Protection Law, and Data Security Law all establish clear protections for user informed consent, data autonomy, and choice rights [34].

However, existing legal frameworks—both domestic and international—often remain principle-oriented and lack clear definitions, technical standards, and operative criteria specific to dark patterns. This leads to ambiguity and enforcement delays in real-world regulation [35]. For example, although GDPR imposes strict consent requirements, it does not clearly define what constitutes a dark pattern, limiting enforcement precision.

To address these challenges, several legal governance strategies are necessary:

Clarification of legal terminology and definitions. Regulatory frameworks should explicitly define “dark pattern design” and its specific variants to enhance enforceability [36] [37]. This process may be supported by the adoption of interface transparency standards such as ISO 9241-210 [38].

Establishment of pre-implementation assessment mechanisms. Regulation should shift from post-hoc punishment to pre-event review. Since dark pattern manipulation often occurs at a subconscious level during user interaction, relying on ex-post accountability cannot effectively restore user losses. Platforms—especially in high-risk domains such as finance, healthcare, and data-intensive services—should be required to undergo interface ethics risk assessments prior to deployment [35].

Strengthening user empowerment mechanisms. This includes requiring platforms to adopt clear language, simplified visual structures, and parallel cancellation paths, while also developing digital literacy education to enhance users’ ability to recognize manipulation, evaluate interface cues, and make autonomous decisions.

5.2. Ethical Measures

Within the digital platform governance system, ethical measures are increasingly

becoming an important complement to legal regulation. Several countries have begun exploring institutionalized ethical constraints on dark patterns. For example, the United Kingdom's Information Commissioner's Office introduced the Age Appropriate Design Code, which, based on the protection of minors' rights, requires interface designs to avoid default push mechanisms and prohibits the use of encouraging or manipulative language, thereby emphasizing respect for user autonomy [39]. Similarly, in 2022, the New Zealand Privacy Commissioner launched the Digital Ethics Lab initiative, promoting interdisciplinary collaboration to evaluate platform design ethics and requiring platforms to explain the intentions behind interface design and its influence on user behavior [40]. These policy developments show that ethical governance should not focus solely on post-hoc penalties but should instead emphasize embedded responsibility in the design stage and the preemptive protection of user rights.

In China, ethical governance of interface design is also gaining attention. The Provisions on the Governance of the Online Information Content Ecosystem (2020) require internet service providers to establish mechanisms for human oversight and user autonomy to prevent over-consumption, addiction, and user rights infringement [41]. The Administrative Provisions on Internet User Public Account Information Services (2021) prohibit misleading distribution mechanisms and require platforms to avoid practices such as "click-bait inducement" or false recommendation displays [42]. In addition, the 2023 directive Notice on Improving Mobile Internet Application Service Capabilities mandates that services such as automatic renewal must not be pre-selected or force-bundled, and that applications must provide clear and accessible exit paths [43]. Although these policies do not explicitly use the term dark patterns, they already address core issues such as inducement-based design, technical manipulation, and forced bundling.

However, both domestic and international ethical norms in interface design have historically focused more on commercial platforms and have not sufficiently addressed public services and social applications. Existing frameworks tend to remain at the macro-principle level, with limited focus on concrete design practices, algorithmic mechanisms, and differentiated effects across groups. Furthermore, the ethical implications of dark patterns vary significantly across social groups, disproportionately affecting the elderly, adolescents, individuals with lower educational attainment, and linguistic minorities.

Given these challenges, ethical governance of dark patterns should include the following measures:

First, introduce ethical risk assessment systems across multiple digital platform domains. Before deployment, digital products—beyond commercial platforms and including public and social service systems—should undergo a behavioral impact assessment, conducted by multidisciplinary ethics review committees that evaluate manipulative potential, risk exposure, and user controllability.

Second, strengthen explainable interface design. Platforms should provide clear semantics, design rationales, and risk explanations regarding interface and algorithmic operations. Moreover, before the platform is put into use, independent

evaluators should assess whether interface information is cognitively accessible to users of different ages and educational backgrounds [44].

Third, promote standardization of ethical norms. International standards bodies (e.g., ISO, W3C) or national regulatory agencies could develop a Digital Interface Design Ethics Standard to regulate practices including default selections, hidden rejection pathways, and emotionally manipulative language [45]. Ethical design education and professional codes of conduct—such as those promoted by ACM SIGCHI—should be integrated into designer training to strengthen accountability at the source of interface creation [46].

5.3. Technical Measures

In international contexts, the technical governance of dark pattern design has increasingly emphasized standardization and tool-based detection, with the primary aim of improving recognition capabilities and supporting corresponding legal and ethical oversight. For example, researchers have proposed the Dark Pattern Analysis Framework, which categorizes and standardizes existing design strategies and identifies 68 distinct types. However, current detection tools are capable of identifying fewer than half of these types, and the scope of existing datasets remains limited—suggesting that the complexity of dark patterns still exceeds current technical recognition capabilities [47]. Similarly, some scholars have introduced artificial intelligence into interface analysis. The AidUI system integrates computer vision and natural language processing to detect more than ten forms of dark patterns in interface screenshots [48]. The AppRay system draws upon a large repository of dark pattern cases and demonstrates strong potential in detection performance [49].

In China, increasing attention is also being paid to the identification and detection of dark pattern design. Scholars have systematically classified dark patterns in e-commerce and financial platforms, providing conceptual foundations for future detection tools. Furthermore, during the 2021 nationwide technical inspection, the Ministry of Industry and Information Technology reported that several mobile applications contained “forced permissions” and “path obstacles,” and subsequently issued public notices or removal orders against non-compliant platforms [50]. Research and development of automated detection systems for dark patterns are currently underway.

However, with the advancement of affective computing, immersive interface design, and generative AI, interface manipulation is becoming increasingly micro-scale and adaptive, raising the difficulty of technological governance. To address these challenges, several strategies should be adopted:

First, develop interaction assistance tools and dark pattern detection systems. Platforms may design browser extensions or interface overlays that highlight default settings, path barriers, or visual inducement elements in real time. Additionally, generative AI and natural language processing models may be employed to construct automated detection frameworks, transforming algorithmic capabilities

into cognitive support tools for users. For example, Mills and Whittle (2023) propose a detection system based on language generation models capable of identifying visual emphasis, terminological ambiguity, and procedural obstruction in interface design [51].

Second, promote multi-stakeholder co-governance by integrating technical evaluation, public oversight, and ethical deliberation. This may include establishing multidisciplinary design review committees involving user representatives, ethicists, and legal advisors to conduct behavioral impact assessments [52].

Third, strengthen public digital literacy education. Educational and public service systems should train users to recognize dark pattern strategies and interface manipulation techniques, improving their sensitivity to and resistance against technological influence [53] [54]. Practical challenges remain, including the rapid evolution of design technologies, cross-jurisdictional inconsistencies, and contextual variations in manipulation perception.

5.4. Conclusions

Dark pattern design is a specialized form of interface manipulation driven by algorithms and behavioral guidance mechanisms. By leveraging default settings, visual cues, and path architecture, digital platforms construct a decision-making environment that appears voluntary yet is covertly controlled. This design has widespread implications across e-commerce, finance, education, healthcare, and social interaction domains, resulting in infringements on user interests, cognitive interference, and privacy exposure.

Therefore, a comprehensive governance framework must be established combining legal, ethical, and technical measures. Key governance directions include: Clarifying legal definitions; Establishing ex-ante evaluation mechanisms; Enhancing user empowerment; Implementing ethical risk review systems; Strengthening explainable interface design; Promoting ethical standardization; Developing automated detection tools; Supporting participatory design governance; And advancing public digital literacy education. These efforts together will support the construction of a fair, transparent, and user-centered digital society.

Acknowledgements

This research was supported by the Inner Mongolia Autonomous Region First-Class Discipline Scientific Research Special Project (Grant No. YLXKZX-NSD-064) and the Graduate Research Innovation Fund of Inner Mongolia Normal University (Grant No. CXJJS25043).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

- [1] Johnson, J. (2014) *Designing with the Mind in Mind: Simple Guide to Understanding*

User Interface Design Guidelines. Morgan Kaufmann.

- [2] Thaler, R.H. and Sunstein, C.R. (2008) *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Yale University Press.
- [3] Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M., *et al.* (2019) Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction*, **3**, 1-32. <https://doi.org/10.1145/3359183>
- [4] Gray, C.M., Kou, Y., Battles, B., Hoggatt, J. and Toombs, A.L. (2018) The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Montreal, 21-26 April 2018, 1-14. <https://doi.org/10.1145/3173574.3174108>
- [5] Li, Q. (2023) Legal Regulation of Dark Patterns on Online Platforms: From Contractual Autonomy and Fundamental Rights to Fiduciary Duties. *Journal of Shanghai University of Political Science and Law*, **38**, 103-118.
- [6] Yang, F. (2022) Legal Regulation of Abusive Dark Patterns in E-Commerce. *China Business and Market*, **36**, 40-50.
- [7] Liu, Y. and Liu, J. X. (2024) Legal Regulation of Dark Patterns in the Digital Economy: Principles, Foreign Experiences and Domestic Pathways. *Journal of Shanghai University of Finance and Economics*, **26**, 122-138.
- [8] Brignull, H. (2010) Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff. <https://www.darkpatterns.org/>
- [9] Kennedy, R. (2020) The Rule of Law and Algorithmic Governance. In: Barfield, W., Ed., *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, 209-232. <https://doi.org/10.1017/9781108680844.012>
- [10] Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W. and Wilson, C. (2021) A Comparative Study of Dark Patterns across Web and Mobile Modalities. *Proceedings of the ACM on Human-Computer Interaction*, **5**, 1-29. <https://doi.org/10.1145/3479521>
- [11] Rakovic, I. and Inal, Y. (2023) Dark Finance: Exploring Deceptive Design in Investment Apps. In: Abdelnour Nocera, J., Kristín Lárusdóttir, M., Petrie, H., Piccinno, A. and Winckler, M., Eds., *Lecture Notes in Computer Science*, Springer Nature, 339-348. https://doi.org/10.1007/978-3-031-42280-5_20
- [12] Sheil, A., Acar, G., Schraffenberger, H., Gellert, R. and Malone, D. (2024) Staying at the Roach Motel: Cross-Country Analysis of Manipulative Subscription and Cancellation Flows. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, Honolulu, 11-16 May 2024, 1-24. <https://doi.org/10.1145/3613904.3642881>
- [13] Fricker, M. (2007) *Epistemic Injustice: Power and the Ethics of Knowing*. Oxford University Press.
- [14] Xiang, C. and Lu, X. (2024) Digital Addiction: Mechanisms, Risks and Regulatory pathways. *E-Government*, No. 12, 108-120.
- [15] Tiemessen, M., Schraffenberger, M. and Acar, Y. (2023) Identifying Dark Patterns in User Account Disabling Interfaces. *Proceedings on Privacy Enhancing Technologies*, **2023**, 321-338.
- [16] Oxera (2021) Bits of Advice: The True Colours of Dark Patterns. <https://www.oxera.com/insights/agenda/articles/bits-of-advice-the-true-colours-of-dark-patterns/>
- [17] Norman, D. (2013) *The Design of Everyday Things*. Basic Books.
- [18] Eslami, M., Rickman, A., Vaccaro, K., *et al.* (2015) Reasoning about Invisible Algorithms in News Feeds. *Conference on Human Factors in Computing Systems*, Seoul,

- 23 April 2015, 153-162.
- [19] Solove, D.J. (2013) Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, **126**, 1880-1903.
- [20] Willis, L. (2020) Deception by Design. *Harvard Journal of Law & Technology*, **34**, 132-133.
- [21] Global Privacy Enforcement Network (2024) GPEN Sweep 2024: Deceptive Design Patterns Report.
https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27_0.pdf
- [22] Norwegian Consumer Council (2021) You Can Log Out, But You Can Never Leave.
<https://storage02.forbrukerradet.no/media/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf>
- [23] European Insurance and Occupational Pensions Authority (2023) Dark Patterns in Insurance.
https://www.eiopa.europa.eu/tools-and-data/behavioural-insights-insurance-and-pensions-supervision/dark-patterns-insurance-practices-exploit-consumer-biases_en
- [24] Kuntsman, A., Miyake, E. and Martin, S. (2019) Re-Thinking Digital Health: Data, Appisiation and the (im)possibility of 'Opting Out'. *Digital Health*, **5**, 1-17.
<https://doi.org/10.1177/2055207619880671>
- [25] Binns, R., Lyngs, U., Van Kleek, M., *et al.* (2018) Perceptions of Justice in Algorithmic Decisions. CHI '18. arXiv:1801.10408.
- [26] Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L. (2020) Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu, 25-30 April 2020, 1-13. <https://doi.org/10.1145/3313831.3376321>
- [27] King, J. and Stephan, A. (2021) Dark Patterns and the Design of Consent Interfaces. *Georgetown Law Technology Review*, **5**, 251-278.
- [28] Mozilla Foundation (2021) Privacy Not Included: Dating Apps Review.
<https://foundation.mozilla.org/>
- [29] Capodivacca, M. and Giacomini, G. (2024) Disciplinary Power in the Digital Age. *Foucault Studies*, **37**, 145-167.
- [30] Gunawan, J., Hartzog, W., Richards, N., *et al.* (2025) Dark Patterns as Disloyal Design. *Indiana Law Journal*, **100**, 1389-1429.
- [31] European Consumer Organisation (2022) Dark Patterns and the EU Consumer Law Acquis.
<https://www.beuc.eu/position-papers/dark-patterns-and-eu-consumer-law-acquis>
- [32] California State Legislature (2018) California Consumer Privacy Act (CCPA)
<https://law.justia.com/codes/california/code-civ/division-3/part-4/title-1-81-5/>
- [33] Cyberspace Administration of China (2021) Provisions on Algorithmic Recommendation Management.
- [34] National People's Congress of China (2021) Personal Information Protection Law.
- [35] Liao, L.H. and Huang, S.L. (2025) Reconstructing the Regulation of Private Power: Logical drivers And Governance Paths of Dark Patterns. *Journal of Hefei University of Technology (Social Sciences)*, **39**, 49-60.
- [36] OECD (2022) Dark Commercial Patterns. OECD Digital Economy Papers No. 336.

- [37] Federal Trade Commission (2022) Bringing Dark Patterns to Light. <https://www.ftc.gov/reports/bringing-dark-patterns-light>
- [38] ISO (2019) ISO 9241-210: Ergonomics of Human-System Interaction—Part 210: Human-Centered Design.
- [39] European Commission (2021) Artificial Intelligence Act Proposal. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>
- [40] Office of the Privacy Commissioner of New Zealand (2022) Digital Ethics Lab Project: Design for Trust. <https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Insights-reports/Privacy-Awareness-and-Engagement-in-New-Zealand-Insights-Report-May-2022.pdf>
- [41] Cyberspace Administration of China (2020) Provisions on the Governance of the Online Information Content Ecosystem.
- [42] Cyberspace Administration of China (2021) Provisions on the Management of Public Account Information Services.
- [43] Ministry of Industry and Information Technology of China (2023) Notice on Improving Mobile Internet Application Service Capabilities.
- [44] Susser, D., Roessler, B. and Nissenbaum, H. (2019) Online Manipulation: Hidden Influences in a Digital World. *Georgetown Law Technology Review*, 4, 1-45.
- [45] W3C (2021) Ethical Web Principles Working Draft. <https://www.w3.org/TR/ethical-web-principles/>
- [46] Association for Computing Machinery (2018) ACM Code of Ethics and Professional Conduct. <https://www.acm.org/code-of-ethics>
- [47] Nie, L., Zhao, Y., Li, C., *et al.* (2024) A Comprehensive Study on Dark Patterns: DPAF Framework. arXiv.
- [48] Mansur, S.M.H., Salma, S., Awofisayo, D.A. and Moran, K. (2023) AidUI: Toward Automated Recognition of Dark Patterns. arXiv.
- [49] Chen, J., Wang, Z., Sun, J., *et al.* (2024) Detecting Dark Patterns in Mobile Apps. arXiv.
- [50] Ministry of Industry and Information Technology of China (2022) Notice on Special Rectification of User Rights Violations.
- [51] Mills, S. and Whittle, R. (2023) Detecting Dark Patterns Using Generative AI: Some Preliminary Results. *SSRN Electronic Journal*, 33 p. <https://doi.org/10.2139/ssrn.4614907>
- [52] Wu, L.R., Li, J.J. and Qi, J.Y. (2025) Theoretical Evolution and Practice Framework of Large Language Model Risk Governance. *E-Government*, No. 9, 54-63.
- [53] OECD (2019) Going Digital: Shaping Policies, Improving Lives. <https://www.oecd.org/digital/going-digital/>
- [54] OECD (2020) The OECD Digital Government Policy Framework. OECD Publishing.