

Rechtsidee

Vol. 14 No. 1 (2026): June
DOI: 10.21070/jihr.v14i1.1149



RECHTSIDEE

PUBLISHED BY
UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

ISSN 2443-3497
(online)



SCAN ME

Rechtsidee

Vol. 14 No. 1 (2026): June
DOI: 10.21070/jihr.v14i1.1149

Table Of Contents

Journal Cover	1
Author[s] Statement	3
Editorial Team	4
Article information	5
Check this article update (crossmark)	5
Check this article impact	5
Cite this article.....	5
Title page	6
Article Title	6
Author information	6
Abstract	6
Article content	7

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Copyright © Author(s). This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licenses/by/4.0/legalcode>

EDITORIAL TEAM

Editor in Chief

Mochammad Tanzil Multazam, Universitas Muhammadiyah Sidoarjo, Indonesia

Scopus ID: [57200559335](#)

Researcher ID: [A-2135-2016](#)

ORCID: [0000-0002-6373-1199](#)

Managing Editor

Dr. Rifqi Ridlo Phahlevy, Universitas Muhammadiyah Sidoarjo, Indonesia

Scopus ID: [57205880567](#)

ORCID: [0000-0002-6684-1190](#)

Editorial Board

Regional Editor for Central Asia

Saydaxmedov Umid Murodovich, Associate Professor of Economic Law, Higher School of Judges under the Supreme Council of Judges of the Republic of Uzbekistan [[Google Scholar](#)]

Esanov Azamat Esirgapovich, Tashkent State University of Law, Uzbekistan [[Scopus](#)]

Dametken Medikhanovna Turekulova, Esil University, Kazakhstan [[Scopus](#)]

Regional Editor for Asia Pacific

Faizal Kurniawan, Universitas Airlangga, Indonesia [[Google Scholar](#)] [[Scopus](#)]

M. Zulfa Aulia, Universitas Jambi, Indonesia [[Google Scholar](#)] [[Scopus](#)]

Fradhana Putra Disantara, Institut Teknologi Bisnis Yadika, Indonesia [[Google Scholar](#)] [[Scopus](#)]

Dr. Noor Fatimah Mediawati, Universitas Muhammadiyah Sidoarjo, Indonesia [[Google Scholar](#)] [[Scopus](#)]

Regional Editor for America

Dinara F. Abdunayimova, University of Illinois College of Law, USA [[Google Scholar](#)]

Regional Editor for Middle East

(No data provided)

Complete list of editorial team ([link](#))

Complete list of indexing services for this journal ([link](#))

How to submit to this journal ([link](#))

Rechtsidee

Vol. 14 No. 1 (2026): June
DOI: 10.21070/jihr.v14i1.1149

Article information

Check this article update (crossmark)



Check this article impact (*)



Save this article to Mendeley



(*) Time for indexing process is various, depends on indexing database platform

Legal Protection for Consumers in the Context of Dark Patterns in Indonesian Marketplace Applications: A Comparative Study With the Netherlands

Annisa Annisa, nisaani614@gmail.com (*)

Program Studi Ilmu Hukum, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia

Sylvana Murni Deborah Hutabarat, sylvana.hutabarat@upnvj.ac.id

Program Studi Ilmu Hukum, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia

(*) Corresponding author

Abstract

General Background: The rapid expansion of digital marketplaces has increased consumer exposure to manipulative interface design, creating new challenges for consumer autonomy, fairness, and legal protection. **Specific Background:** In Indonesian marketplace applications, dark patterns appear through false urgency, hidden costs, sneak into basket, fake reviews, fake discounts, and disguised advertisements, which may harm consumers psychologically and financially. **Knowledge Gap:** Indonesia's current legal framework remains general, fragmented, and reactive, while no specific regulation explicitly defines or prohibits manipulative interface design in marketplace ecosystems. **Aims:** This normative legal study examined consumer protection against dark patterns in Indonesia and compared it with Dutch regulations through statutory, conceptual, and comparative approaches. **Results:** Indonesian law only partially addresses dark patterns through consumer protection, electronic information, personal data, and electronic commerce provisions. By contrast, the Netherlands applies multi-layered protection through the DSA, WHC, GDPR-related standards, ACM technical guidelines, and proactive monitoring, including automated screening tools. **Novelty:** This study specifically compares Indonesia and the Netherlands in regulating and enforcing consumer protection against marketplace dark patterns. **Implications:** Indonesia needs explicit dark pattern regulation, operational technical guidelines, technology-based monitoring, stronger supervisory institutions, and targeted digital literacy programs to protect consumers from manipulative marketplace interfaces.

Highlights:

- Marketplace users face psychological and financial harm.
- The national framework remains general and complaint based.
- ACM guidance demonstrates proactive technical supervision and automated screening.

Keywords: Dark Patterns, Consumer Protection, Marketplace Applications, Regulation

Published date: 2026-06-23

Introduction

In this rapidly evolving digital age, there has been a fundamental and significant shift in consumer patterns and behavior. Digitalization has transformed the way we communicate, conduct transactions, and access information. The digital transformation has spurred the emergence of various online application based business innovations that offer users great convenience and efficiency [1]. E-commerce has become a cornerstone of Indonesia's digital economy, accounting for 73% of the total value of the national digital economy and projected to continue growing to reach USD 150 billion by 2030. Bank Indonesia reports rapid growth in the national e-commerce ecosystem, with the value of digital transactions in 2024 reaching Rp 487 trillion and exceeding 3.71 billion transactions. E-commerce transactions are projected to continue growing by 3.3% to reach Rp 503 trillion in 2025 [2]. Although this makes it easier for consumers to shop online on marketplaces platforms, there are also drawback that could potentially harm buyers, meaning that these technological advancements present new challenges for consumer protection in the digital space, this technology is often difficult to monitor and raises concerns about transparency, fairness in transactions, and the potential misuse of personal data [3].

Amid the highly competitive digital marketplaces, many businesses on these platforms are not only innovating in their services and products but are also vying to capture consumers attention through various interface design strategies on marketplace applications to influence their behavior. One strategy that has recently garnered global attention is the use of dark patterns. The practice of dark patterns was first introduced by a UX designer named Harry Brignull in 2010. According to him, dark patterns are subtle tricks embedded in websites or apps to make users do things they don't actually want to do [4]. According to the Organization for Economic Cooperation and Development (OECD), "dark patterns" are business practices that exploit elements of digital architecture particularly in the design of online interfaces to undermine or interfere with consumer autonomy, decision making, or choice. These practices often deceive, coerce, or manipulate consumers and are likely to cause direct or indirect harm to consumers [5]. The European Data Protection Board Guidelines 03/2022 (EDPB) define dark patterns as interface designs and user experiences that are intentionally crafted to lead users to make decisions they do not actually want and that may even be harmful to them all done covertly to influence user behavior [6].

Dark patterns in Indonesia typically take the form of hidden costs, false urgency, deceptive pricing, products automatically added to the cart, disguised ads, manipulation of reviews and ratings, and so on [2]. Such practices have the potential to exploit consumers cognitive biases such as scarcity bias and urgency bias thereby prompting purchases without rational consideration, directly distorting decision-making, creating information asymmetries, and resulting in financial losses [7]. This issue places consumers in online marketplaces in a vulnerable position. In Indonesia, regulations regarding consumer protection in the digital context remain general in nature and do not yet comprehensively address dark patterns. Existing regulatory instruments include Law No. 8 of 1999 on Consumer Protection (UUPK), Law No. 1 of 2024 on the Second Amendment to the Law on Information and Electronic Transactions (ITE Law), Law No. 27 of 2022 on Personal Data Protection (PDP Law), Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions (PSTE Regulation), and Government Regulation No. 80 of 2019 on Trade via Electronic Systems (PMSE Regulation).

Existing regulations only partially address certain aspects of dark patterns, with none explicitly regulating manipulative practices in user interface design. Current approaches tend to focus on the parameter of "misleading information" rather than prohibiting manipulative interface design itself. As reflected in Articles 7(a), 7(b), 9, and 10 of the UUPK regarding the obligation of business actors to act in good faith, provide accurate, clear, and honest information, and the prohibition against business actors engaging in misleading promotions. The existing provisions do not address how the interface design should be presented; they focus only on the substantive content of the information [8]. Furthermore, Articles 15 and 28 (1) of the ITE Law stipulate that Electronic System Operators (ESOs) are required to operate systems reliably and securely, are responsible for the proper functioning of electronic systems, and are prohibited from disseminating false information that causes material harm to consumers. Article 20 (2) (a) of the PDP Law stipulates that consent must be given validly and explicitly, while manipulation through interface design can undermine the user's freedom and awareness in giving consent. Furthermore, Article 29 (f) of the PSTE Regulation requires PSE to provide information to users regarding the procedures for reaching an agreement; however, this provision does not specifically regulate the process of reaching an agreement in electronic transactions without using manipulative methods that could influence users in making decisions. Furthermore, Articles 13 and 39 of the PMSE Regulation require transparency regarding technical details and terms of sale, but do not address ethical aspects in the application's interface [8].

This raises concerns about the weakness of legal protection, which leaves consumers more vulnerable to harmful practices in the absence of adequate oversight and enforcement mechanisms. This situation creates a legal gap, primarily due to the absence of an explicit ban on interface design manipulation, the lack of a regulatory body with a specific and proactive mandate to address these issues, and the unavailability of technical operational guidelines for law enforcement and businesses in the digital space. There is a stark contrast when examining the approach of the European Union, particularly the Netherlands. Through the Digital Services Act (DSA), it has explicitly prohibited interface design practices that deceive users in data collection and digital transactions. Article 25(1) of the DSA explicitly states that online platform operators must not design, configure, or operate their online interfaces in a way that deceives or manipulates service recipients, or in a way that materially alters or impairs their ability to make autonomous and informed decisions. This prohibition is reinforced by Recital 67 of the DSA, which provides definitions and examples of dark pattern practices, including presenting options in a non-neutral manner, making service cancellation procedures significantly more difficult than registration, and using default settings that are biased toward the platform provider's interests. Thus, the DSA establishes both ethical and legal standards for digital design integrity, and views dark patterns as violations of the principles of transparency and consumer protection in the digital space [9]. Subsequently, Directive 2005/29/EC (Unfair Commercial Practices Directive/UCPD), implemented through Book 6 of the Civil Code and the Consumer Protection Enforcement Act (WHC), served as the initial foundation,

which was further strengthened by the General Data Protection Regulation (GDPR/Regulation (EU) 2016/679) regarding the protection of personal data. At the national level, the Netherlands enacted the Digital Services Regulation Implementation Act (UDV) through the Act of January 29, 2025, Staatsblad 2025, No. 21, which designates the Autoriteit Consument en Markt (ACM) as the primary independent supervisory authority. ACM has not only issued technical guidelines regarding dark patterns but has gone a step further by developing an automated scanning tool capable of detecting dark pattern practices without relying solely on consumer reports [10]. This is something that Indonesian consumer protection agencies currently lack. The legal gap between Indonesia and the Netherlands lies in a difference in paradigms. Indonesia tends to respond only to violations that have already occurred. Meanwhile, regulations in the Netherlands take a more proactive approach by governing how user interfaces are designed to prevent the manipulation of consumer choices.

A study by Supriyanto and Molid Nurman Hadi (2025) titled "Analysis of Dark Pattern Mitigation in E-Commerce" examines the potential losses incurred by consumers due to dark pattern practices and a lack of oversight in Indonesian e-commerce, using a qualitative descriptive approach through literature review and benchmarking against the European Union, South Korea, and India. Meanwhile, the study reviewed by the author employs a normative legal methodology and specifically compares regulations and their implementation between Indonesia and the Netherlands. A study by Sylviana, Maharani, and Wibowo (2025), titled "The Validity of Dark Patterns in Obtaining Consent for Personal Data Processing in Indonesia," examines the validity of regulations regarding dark patterns in obtaining consent for personal data processing under the Personal Data Protection Act (PDP Act).

Based on the above, this study is important to, first, examine and analyze legal regulations regarding dark pattern practices in marketplace applications in Indonesia based on applicable provisions, and second to compare legal regulations and enforcement regarding dark pattern practices in marketplace applications between Indonesia and the Netherlands. The results of this study are expected to provide normative recommendations for improving national legal policies to be more adaptive to consumer protection issues in the digital era. Based on the above, the author is interested in conducting further research on the topic "Legal Protection for Consumers in the Context of Dark Patterns in Indonesian Marketplace Applications: A Comparative Study with the Netherlands"

Method

In this study, the author employs a normative legal research method focused on analyzing positive legal norms regarding consumer protection against dark patterns in marketplace applications. This approach examines existing regulations as the primary basis for resolving legal issues, including regulatory gaps in Indonesia, and compares them with the Dutch regulatory framework. This study employs a statutory approach that focuses on examining written legal rules (the constitution, laws, government regulations, and other implementing regulations) as the primary source. The Conceptual Approach analyzes legal concepts such as consumer autonomy, good faith, and regulatory gaps as an evaluative framework for assessing dark pattern practices and the Comparative Approach compares norms, institutions, or rulings across two or more jurisdictions to identify similarities, differences, and best practices. This approach is useful for assessing whether the domestic legal framework is consistent or needs to be adapted based on the experiences of other countries [11]. The legal materials used are primary legal sources, including Indonesian legislation (UU PK, UU ITE, UU PDP, PP PSTE, PP PMSE), European Union regulations that apply directly (GDPR Regulation EU 2016/679; DSA Regulation EU 2022/2065); Dutch national implementing legislation (Wet handhaving consumentenbescherming, Stb. 2006, 591; Uitvoeringswet Digitaal dienstenverordening, Stb. 2025, no. 21). Secondary legal materials include legal textbooks, academic journals; OECD Report on Dark Commercial Patterns (2022); UCPD Directive 2005/29/EC; ACM Guidelines on the Protection of the Online Consumer (2022); EDPB Guidelines 03/2022 on Deceptive Design Patterns.. Tertiary legal materials consist of legal dictionaries and encyclopedias.

Result and Discussion

A. Legal Regulation on the Use of Dark Patterns in Marketplace Applications in Indonesia

1. Types of Dark Patterns in Indonesian Marketplaces

First, false urgency is one of the most common dark patterns found on Indonesian marketplaces. This practice involves displaying a countdown timer on promotional offers that does not reflect the actual time limit, as well as fabricated notifications that stock is running low. On platforms like Shopee, Lazada, and Tokopedia, the 'Flash Sale' feature designed to appear as though it lasts only a few hours, yet similar promotions are available continuously every day is a clear example of scarcity bias manipulation that exploits consumers' psychological vulnerabilities to influence impulsive purchases. Second, hidden costs/drip pricing are dark patterns with the most direct financial impact. In practice, during the purchasing process, consumers are shown an attractive base price, but at checkout, various additional fees such as service charges or other handling fees are only revealed at the end. Third, "sneak into basket" involves automatically adding products to the shopping cart without the consumer's knowledge or consent. Fourth, fake reviews & testimonial manipulation the practice of manipulating reviews on marketplaces is becoming increasingly prevalent, ranging from the use of bots to create instant positive testimonials to the unilateral removal of negative reviews by the platform. This practice creates a positive product image by showing buyers only the positive aspects while hiding genuine reviews. Fifth fake discounts, during Harbolnas, the Indonesian Consumers Foundation (YLKI) frequently finds that product prices are first inflated before a discount is applied only after the price is raised is a discount offered. This practice amounts to deceiving consumers because the final price

turns out to be the same as or even higher than the original price [2]. Sixth, disguised advertisements are a form of dark patterns on marketplaces designed to exploit consumers by disguising paid ads as navigation or organic information. Research conducted on marketplace platforms in Indonesia shows that although users are exposed to these manipulative practices, not all are able to recognize them due to factors such as unclear interface information and user trust in the platform [12].

2. Legal Framework for Consumer Protection Regarding Dark Patterns in Indonesia

a. Law No. 8 of 1999 on Consumer Protection

Legal regulations regarding dark patterns in marketplace applications in Indonesia have not yet been explicitly addressed within a specific regulatory framework; instead, they are scattered across various laws and regulations that are only partially related. This situation indicates that Indonesia's legal system still employs a general approach in regulating business conduct in the digital space, and thus has not yet been able to comprehensively address the complexity of manipulation practices based on interface design. The Consumer Protection Law (UUPK) is the most fundamental legal instrument for consumer protection; Article 4(c) of the UUPK states "the right to accurate, clear, and truthful information regarding goods and/or services." Dark patterns, in principle, violate this right by concealing or presenting information in a design layout that causes consumers to make decisions without complete information [13]. Hidden costs that are only disclosed at the final stage of payment, and disguised advertisements that masquerade as unpaid content, constitute a clear violation of the rights guaranteed by this article. Furthermore, Article 7(a) of the UUPK requires business operators to act in good faith in conducting their business, while Article 7(b) of the UUPK mandates the provision of accurate, clear, and honest information [14]. Marketplace operators who employ dark patterns in the design of their application interfaces are failing to fulfill both of these obligations. Furthermore, Article 9(1) (a) of the UUPK prohibits business operators from offering, promoting, or advertising goods and/or services in a misleading manner, and or as if such goods have met certain criteria and/or are subject to a discount, such as using exaggerated language in advertisements that contain promises whose truthfulness is uncertain [15]. The practice of dark patterns (fake discounts), which displays prices that do not reflect actual market prices, directly violates this provision. Article 10 of the UUPK pertains to the prohibition on business entities from offering, promoting, advertising, or making false or misleading statements. The practice of false urgency (fake countdowns) constitutes a deceptive act, as it creates a false sense of urgency or artificial conditions to distort decision-making and trigger impulsive consumer purchases. Article 18(2) of the UUPK prohibits business operators from including standard clauses whose placement or format is difficult to understand or clearly visible. In the context of dark patterns, this provision applies to manipulative consent interface practices such as options pre-checked by the system, consent text that is intentionally obscured, or a "decline" button that is deliberately hidden all of which constitute standard clauses that are not transparently disclosed. Article 62(1) of the UUPK states that business entities violating the provisions of Articles 9, 10, and 18 shall be punished by imprisonment for a maximum of 5 (five) years or a fine of up to Rp 2,000,000,000.00 (two billion rupiah). The UUPK, as a special regulation for consumer protection, was enacted in 1999 before the digital era, and therefore does not specifically address consumer issues in digital transactions on marketplaces [16]. Article 45 (2) of the UUPK provides for the resolution of consumer disputes through both judicial and extrajudicial channels, depending on the agreement between the parties. However, these mechanisms have not yet functioned optimally in addressing cases involving dark patterns. In many situations, consumers are unaware that the decisions they make are actually influenced or guided by manipulative digital design. As a result, consumers often do not realize that they have grounds to file a complaint or pursue dispute resolution through the mechanisms provided.

b. Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions

Article 15(1) of the ITE Law requires PSE to operate Electronic Systems reliably and securely and to be responsible for ensuring that Electronic Systems operate as intended. This regulation is technical in nature; its primary focus is to ensure that electronic systems operate reliably and are secure from threats, such as hacking. It does not address the integrity of interface design regarding the potential for manipulation of users by the platform itself. Furthermore, Article 28(1) of the ITE Law pertains to the prohibition of spreading false and misleading information that results in consumer losses in Electronic Transactions. The penalty is set forth in Article 45A(1) of the ITE Law, "Any person who intentionally disseminates false and misleading information that harms consumers in Electronic Transactions shall be punished by imprisonment for a maximum of 6 (six) years and/or a fine of up to Rp1,000,000,000.00 (one billion rupiah). This rule can actually be applied to several dark pattern practices, one of which is false urgency (fake countdown timers), since the display of a fake timer can be considered misleading information and cause harm to consumers. However, enforcement remains difficult due to the burden of proving "intentionality," which is hard to establish. Dark patterns typically deceive users subtly through interface design, so they do not always appear as deliberate acts of disseminating false information often going unnoticed by the consumers who fall victim to them [8].

c. Law No. 27 of 2022 on the Protection of Personal Data

In the context of personal data protection, the Personal Data Protection Act (PDP Act) is conceptually relevant to the practice of dark patterns. Article 20 (2) (a) states "Valid and explicit consent from the data subject for one or more specific purposes that have been communicated by the data controller to the data subject." This means that consent must be given validly that is, freely, specifically, with full knowledge, and unambiguously. In the practice of privacy zuckering dark patterns, the consent interface is designed in such a way that users, without realizing it, grant permission far broader than what they actually intend for example, through confusing options, text intentionally made difficult to understand, or an "agree" button that is far more prominent than the optvout option. Furthermore, the absence of prohibitions against the use

of manipulative interface designs creates a legal loophole that can be exploited by data controllers [17].

d. Government Regulation No. 71 of 2019 on Electronic System Operators and Electronic Transactions and Government Regulation No. 80 of 2019 on Commerce via Electronic Systems

Article 29(f) of the PSTE Regulation states that PSE operators are required to provide information to Electronic System Users regarding the procedures for reaching an agreement. In this regard, there are no specific provisions governing the process of reaching an agreement in electronic transactions that prohibit the use of manipulative methods capable of influencing users decision making. The issue is that the widespread practice of dark patterns found in Indonesian marketplaces contradicts the principles of good faith, transparency, and accountability established in Article 45 of the PSTE Regulation. Therefore, existing provisions should be in place to safeguard and protect consumer rights to make decisions independently, without pressure or influence from third parties, so that every choice made reflects the consumer's own will and judgment [9]. Meanwhile, the PMSE Regulation, through Article 13, addresses the obligation of PMSE business operators to provide accurate, clear, and truthful information regarding goods, including the electronic systems used; Article 39(2) addresses the validity and binding nature of electronic offers, provided they are made in good faith, fairly, and in a balanced manner, and within a specified timeframe. These regulations do not yet address the issue of misuse of interface design on marketplace applications. Consequently, without a clear legal basis and guidelines, effective enforcement of oversight and guidance becomes difficult [2].

B. A Comparison of Legal Regulations and Enforcement Application Between Indonesia and the Netherlands

The legal system in place to address dark patterns in the Netherlands, as an EU member state, is multi layered. Each layer of regulation fills the legal gaps left by the others, with the aim of providing comprehensive and integrated consumer protection. These regulations are substantively aligned with the OECD's characterization as outlined in the introduction. The Digital Services Act represents a regulatory framework responsive to the times. Article 25(1) explicitly prohibits online platform operators from designing, configuring, and operating their online interfaces in a manner that deceives or manipulates service users, or in a way that materially alters or impairs their ability to make autonomous and informed decisions. As emphasized in Recital 67 of the DSA, dark patterns are practices that materially distort or impair users' ability to make autonomous and informed choices, whether intentionally or not [18]. The distinctive feature of the DSA lies in its approach, which focuses not only on the content of information provided to consumers but also explicitly regulates the design and functionality of digital interfaces. The DSA also distinguishes different scopes of obligations based on the scale of digital platforms; platforms categorized as Very Large Online Platforms (VLOPs) with at least 45 million monthly active users are under the direct supervision of the European Union as stipulated in Article 56 of the DSA, while platforms with fewer users are supervised by the national authorities of each EU member state [18].

Furthermore, Directive 2005/29/EC on Unfair Commercial Practices Directive (UCPD) has been implemented by the Netherlands into its national law through Book 6 of the Civil Code and the Consumer Protection Enforcement Act. Article 5 of the UCPD prohibits unfair commercial practices; a practice is considered unfair if it materially distorts or is likely to distort the economic behavior of the average consumer reached or targeted regarding a product. Furthermore, Article 6(1) of the UCPD extends this prohibition to misleading practices, even if they contain factually correct information, provided that the presentation of such information leads to a transactional decision by the consumer that the consumer would not have made otherwise, in relation to one or more of the following: (a) the existence or nature of the product; (b) the main characteristics of the product, such as availability, benefits, risks, composition, accessories, after-sales service, complaint handling, method and date of manufacture or provision, delivery, suitability for use, use, quantity, specifications, geographical or commercial origin, or the expected results of its use; (c) the scope of the trader's commitments, the motives behind commercial practices, and the nature of the sales process; (d) the price or method of price calculation, or the existence of specific price advantages" [19]. Annex I of the UCPD contains a blacklist of practices that are absolutely prohibited; forms of dark patterns such as false urgency, hidden costs, disguised ads, etc., can be addressed through these provisions. However, the UCPD has inherent limitations when dealing with increasingly sophisticated contemporary dark patterns. In a European Parliament resolution in December 2023, the Parliament explicitly called on the European Commission to close existing regulatory gaps and strengthen transparency provisions, as current rules are deemed insufficient to effectively mitigate the negative impacts of dark pattern practices [19]. These limitations subsequently led to the creation of the DSA as a regulation that is more responsive to dark patterns.

Furthermore, in Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) while dark patterns are not specifically mentioned, several articles directly address such practices. Article 5(1)(a) of the GDPR requires that the processing of personal data be lawful, fair, and transparent. Furthermore, Article 4(11) of the GDPR stipulates that consent must be freely given, specific, informed, and unambiguous. Dark patterns designed to manipulate consumer consent may violate these provisions. Subsequently, the publication of Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them states that "Deceptive Design Patterns" are online interface elements on social media platforms that are intentionally designed to persuade users to make decisions they do not actually want or need and that could be detrimental to them [6].

To ensure the effective enforcement of the DSA at the national level, the Dutch government enacted the Act of January 29, 2025, Staatsblad 2025, No. 21, also known as the Digital Services Act Implementation Act (UDV). The UDV does not recodify the substance of the prohibition on dark patterns, which is already directly regulated in the DSA, but rather serves as a formal legal instrument establishing the institutional structure, division of jurisdiction, and sanctions regime in the

Netherlands. Article 2.1 of the UDV officially designates the Autoriteit Consument & Markt (ACM) as the primary supervisory authority for the oversight of dark patterns in the Netherlands [20]. ACM has also published the Leidraad Bescherming Online Consument (Guidelines for Online Consumer Protection), a technical document that provides concrete guidance to businesses on the implementation of consumer protection rules in the digital space online businesses now have clear guidance on what is prohibited, including guidance on how to avoid dark patterns [21].

The Netherlands has demonstrated tangible oversight of dark pattern practices. ACM uses automated screening tools to scan thousands of marketplace stores and found 41 stores using fake countdown timers. ACM confronted the involved businesses through a pragmatic approach; subsequently, all businesses ceased the practice without formal sanctions being imposed, as the businesses in this case voluntarily complied with ACM's warning [22]. However, if the business in question does not acknowledge the violation after being warned and continues to use such practices, it risks violating Article 6:193g(g) of the Civil Code (BW), which implements the UCPD's "blacklist" provision prohibiting deceptive claims that a product is available only for a limited time, with the aim of pressuring consumers to make a decision quickly without sufficient time to consider. If the business operator fails to comply with the warning, the ACM has the authority to impose a fine pursuant to Article 2.9 in conjunction with Article 2.15(2) of the WHC, up to a maximum of €900,000 or 10% of turnover. This case demonstrates that the ACM's use of automated detection tools makes it possible to detect violations efficiently and on a large scale without relying solely on consumer reports; it also shows that compliance among businesses and service providers can be achieved only through the presence of a credible and proactive regulatory authority.

In 2024, five online stores were found to be using fake discounts on their online interfaces; all five displayed discounted prices with misleading original prices, making it appear as though consumers were getting a good deal when they were not. In this case, ACM imposed administrative fines totaling €621,000 on the five online stores found to have engaged in such practices, with the following breakdown: Day Traders/Koopjedaal at €163,000, Leen Bakker at €130,000, G -Star at €110,000, JYSK at €112,500, and Tommy Hilfiger at €105,500 [23]. The basis for imposing these sanctions refers to Article 2.9 in conjunction with Article 2.15(1) of the WHC. In this context, it is highly relevant to categorize this as a form of dark patterns, particularly the fake discount/misleading pricing typology, as it manipulates consumers' perception of the magnitude and authenticity of the discount. Then, at the European Union level in June 2025, the European Consumer Organisation (BEUC), together with 25 consumer organizations from 21 countries including Consumentbond (the Dutch national consumer organization) formally filed a complaint with the European Commission against SHEIN. The complaint pertains to alleged use of manipulative interface practices (dark patterns) deemed to encourage consumers to make excessive purchases, exceeding their needs or initial intentions. SHEIN is considered the most aggressive marketplace in employing such manipulative practices, utilizing at least eight distinct types of dark patterns. The forms of dark patterns used include limited stock messages such as "Only xx left," fake countdown timers during flash sales, social pressure through reviews or other users' activities, and confirmation shaming techniques such as the question "Sure to leave? you will lose €200 reward?". All of these practices are applied repeatedly, both through the website and the app, including via notifications that continuously appear to consumers [24].

The CPC Network (Consumer Protection Cooperation Network) investigation into SHEIN was led by the competent national authorities of Belgium, France, Ireland, and the Netherlands, with ACM acting as one of the authorities under the coordination of the European Commission. In April 2024, SHEIN was officially designated as a Very Large Online Platform (VLOP) under the DSA after its monthly active user count in the European Union exceeded 45 million. With this designation, SHEIN is subject to all the stricter obligations set forth in the DSA, including transparency obligations, systemic risk mitigation, and user protection on digital platforms. The European Commission sent a Request for Information (RFI) to SHEIN to investigate alleged violations of the DSA. The request for information specifically highlighted several issues, one of which was the use of dark patterns in the marketplace platform's interface. The investigation focuses on the alleged use of addictive design elements and the lack of transparency regarding recommendation algorithms. The case remains under investigation and monitoring as of now; if SHEIN is found to be non-compliant with DSA provisions, it could face fines of up to 6% of its total annual global revenue as stipulated in Article 52 of the DSA [25]. Moreover, under Articles 53 and 54 of the DSA, users of digital platforms who have suffered harm as a result of dark patterns may file complaints through out of court dispute resolution mechanisms designated by European Union member states. These mechanisms provide a more structured and accessible resolution pathway for consumers a feature that is currently lacking in Indonesia's consumer protection system.

Although the term dark patterns itself is not yet recognized in the existing legal system, the fact is that this practice does occur in marketplaces in Indonesia. Legal protection plays a crucial role in ensuring that consumers who experience discrepancies can obtain fair compensation, holding sellers and marketplace platforms accountable, providing effective dispute resolution mechanisms, and building consumer trust in online transactions [26]. The most fundamental difference between the Indonesian and Dutch legal systems in addressing dark patterns actually lies not only in the existence of regulations but also in the legal paradigms employed. Indonesia tends to adopt an information based approach, where the regulatory focus centers on the information provided to consumers. In this approach, a violation is generally assessed based on whether the content of the information is accurate or not. This is evident in Articles 9 and 10 of the Consumer Protection Law, which prohibit businesses from making "misleading" offers. This indirectly implies the assumption that consumer manipulation always occurs through information that is factually incorrect or misleading. Through the DSA and UCPD, the Netherlands is moving toward a design based approach, where the law not only assesses whether the information provided is true or false but also considers how information is presented within the interface design and to what extent it influences consumers freedom to make decisions. Although the term "dark patterns" itself is not yet recognized in existing positive law, the fact is that this practice does occur in marketplaces in Indonesia. According to BPKN records for the 2023–2025 period, there were a total of 3,582 consumer complaints, the majority of which originated from e-commerce. There has been a shift in complaint patterns: while previously many complaints were related to physical products, there are now more complaints

Rechtsidee

Vol. 14 No. 1 (2026): June
DOI: 10.21070/jihr.v14i1.1149

regarding systemic practices such as hidden costs and other dark pattern practices [27]. However, this figure is likely still lower than the actual number of violations, given that most victims of dark patterns are often unaware that their decisions have been influenced or manipulated.

Consumer protection oversight in Indonesia remains fragmented across several agencies, such as the National Consumer Protection Agency (BPKN), the Consumer Dispute Resolution Agency (BPSK), the Business Competition Supervisory Commission (KPPU), and the Ministry of Communication and Digital Affairs (Komdigi). Each agency has different authorities and areas of focus. However, to date, there is no agency that actively monitors, detects, and addresses the use of dark patterns in marketplace applications. This situation contrasts with the Netherlands, which employs a centralized oversight system through a single independent agency the Authority for Consumers and Markets (ACM) enabling more integrated and effective oversight.

Table 1. Comparison of consumer protection against Dark Patterns in Marketplace Applications Between Indonesia and the Netherlands

Aspect	Indonesia	Netherlands
Legal Basis	This has not yet been explicitly regulated; existing regulations are general in nature and do not comprehensively address dark patterns. Existing legal instruments include: - Law No. 8 of 1999 on Consumer Protection (UUPK), - Law No. 1 of 2024 (ITE Law), - Law No. 27 of 2022 on Personal Data Protection (PDP Law), - Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions (PP PSTE), - Government Regulation No. 80 of 2019 on Electronic Commerce (PP PMSE)	The existing regulations are quite comprehensive and integrated, covering: - DSA (Regulation EU 2022/2065), - UCPD (Directive 2005/29/EC) - GDPR (Regulation EU 2016/679), - Wet handhaving consumentenbescherming (WHC), - Uitvoeringswet digitale dienstenverordening (UDV).
Definition & Explicit Prohibition of Dark Patterns	Definition & Explicit Prohibition of Dark Patterns No Indonesian regulation has yet explicitly defined or prohibited manipulative design practices (dark patterns). The UUPK only addresses misleading information (Articles 7, 9)	Recital 67 explicitly defines dark patterns as designs capable of materially distorting or impairing consumers' ability to make autonomous and informed choices, whether intentionally or not, Article 25(1) of the DSA prohibits the use of dark patterns.
Supervisory Authority	The regulatory landscape is fragmented, with no single authority currently overseeing this area, namely: BPKN, BPSK, KPPU, and Komdigi.	- ACM (Autoriteit Consument en Markt) is a single, independent authority at the national level in the Netherlands. - The European Commission, which has the authority to enforce against dark patterns on platforms with 45 million or more monthly active users, known as Very Large Online Platforms (VLOPs), as stipulated in Article 56 of the DSA.
Technical Standards for Dark Patterns	There are no technical guidelines regarding manipulative interface design in marketplaces.	- Leidraad bescherming online consument (ACM Guidelines on Online Consumer Protection) official ACM technical guidelines explaining the application of the WHC to dark patterns in the digital space, used as a compliance assessment standard in ACM investigations [21]. - EDPB Guidelines 03/2022 European Union guidelines on dark patterns based on personal data protection, applicable in all member states, including the Netherlands
Applicable Penalties	There are no explicit provisions governing violations	- Article 2.9 in conjunction with Article 2.15(2) of the WHC provides

Rechtsidee

Vol. 14 No. 1 (2026): June
DOI: 10.21070/jihr.v14i1.1149

	involving manipulative interface design; however, under Article 62 of the UUPK, the penalty is imprisonment for a maximum of 5 years or a fine of up to Rp. 2,000,000,000.00 (two billion rupiah), Article 28(1) of the Electronic Information and Transactions Law (ITE Law) regarding misleading information causing consumer harm in electronic transactions carries a maximum prison sentence of 6 (six) years and/or a fine of up to Rp1,000,000,000.00 (one billion rupiah).	for a maximum fine of €900,000 or 10% of the business operator's turnover.. - DSA Article 52 provides for a maximum fine of 6% of annual turnover.
Supervisory methods	Are still reactive in nature, relying solely on consumer complaints	A more proactive approach involves using automated screening tools in certain cases without waiting for consumer reports.
Dispute Resolution Mechanisms	Under Article 45(2) of the UUPK, disputes may be resolved through court proceedings or alternative dispute resolution, at the discretion of the parties.	Through litigation or alternative dispute resolution under Articles 53 and 54 of the DSA.

Conclusion

Based on the findings of the study outlined above, it can be concluded that the use of dark patterns in marketplace applications in Indonesia has been shown to harm consumers, both psychologically and financially. Indonesia's current legal framework is not yet capable of comprehensively addressing dark patterns. Existing regulations still rely on a general approach focused on proving the textual inaccuracy of information, whereas the essence of dark patterns lies in the presentation of information through interface designs that manipulate user behavior. A comparison with Dutch regulations reveals significant gaps, both in terms of norms and institutional frameworks. The Netherlands has an integrated, multi-layered protection regime that not only explicitly prohibits dark patterns but also establishes consumer autonomy as a protected value. The ACM demonstrates that law enforcement in the digital age cannot rely solely on individual complaint mechanisms but must be proactive and technology driven. Indonesia needs to immediately establish specific regulations that explicitly define and prohibit the use of dark patterns within the marketplaces ecosystem. These provisions can be incorporated through a revision of the UUPK or the issuance of a specific Government Regulation on digital platform interface design that protects consumers. Additionally, operational technical guidelines should be issued to serve as a reference for businesses in designing legally compliant digital interfaces. Indonesia needs to adopt technology based monitoring mechanisms given the nature of dark patterns, which are often unnoticed by consumers. Regarding consumer awareness, the government needs to promote digital literacy programs that specifically equip consumers with the ability to recognize dark pattern practices.

Acknowledgement

The author would like to express her deepest gratitude to everyone who contributed to the research and writing of this article. In particular, the author greatly appreciates the guidance and support of her academic advisor, who consistently provided direction throughout the writing process. The author would also like to thank her beloved family and friends for their unwavering support, which made it possible to complete this work.

References

1. E. P. Pembayun and A. F. Gunawan, "Perlindungan Hukum terhadap Konsumen dalam Transaksi Digital: Tinjauan terhadap Implementasi UU Perlindungan Konsumen Marketplace," *Jurnal Fakta Hukum*, vol. 3, no. 2, pp. 84–94, Mar. 2025, doi: 10.58819/jfh.v3i2.156.
2. Supriyanto and M. N. Hadi, "Analisis Mitigasi Dark Pattern pada E-Commerce di Indonesia," *Trade Policy Jurnal*, vol. 4, no. 1, Dec. 2025, Available: <https://jurnal.kemendag.go.id/index.php/TPJ/article/view/1093/460>
3. R. H. Gultom, N. A. Sinurat, J. A. Sirait, and B. Purba, "Strategi Penguatan Perlindungan Konsumen Digital dalam Transaksi E-Commerce Berbasis Analisis UU Perlindungan Konsumen dan UU ITE di Indonesia," *J-CEKI*, vol. 4, no. 6, pp. 282–293, Sep. 2025, Available: <https://al-haramjournal.id/index.php/J-CEKI/article/view/10088>
4. H. Brignull, "Deceptive Patterns Exposing the Tricks Tech Companies Use to Control You," Jul. 2023, Available: https://uploads-ssl.webflow.com/6412167c874d3b52f2a4d962/64c22582d9517897c6376a2b_Deceptive-Patterns-Sample-Chapters-27-July-2023.pdf
5. OECD, "Dark Commercial Patterns OECD Digital Economy Papers," Oct. 2022, Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf
6. EDPB, "Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them Version 2.0," 2023, Available: https://www.edpb.europa.eu/system/files/2023-02/edpb_03%202022_guide
[ISSN 2443-3497 \(online\)](https://www.edpb.europa.eu/system/files/2023-02/edpb_03%202022_guide), <https://rechtsidee.umsida.ac.id>, published by [Universitas Muhammadiyah Sidoarjo](https://www.umsida.ac.id)

Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

lines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

7. I. Nyoman Susipta, "Dark Patterns dalam Digital Marketing: Etika dan Dampaknya terhadap Loyalitas Konsumen," *International Journal of Economics and Management Research*, vol. 4, no. 1, pp. 583–590, Apr. 2025, doi: 10.55606/ijemr.v4i1.324.
8. P. N. Az-Zahra', N. Nurlaily, and A. Agustianto, "Regulating Dark Patterns in Indonesian E-Commerce: Comparative Lessons from South Korea and the EU," *Journal of Judicial Review*, vol. 27, no. 2, Dec. 2025, doi: 10.37253/jjr.v27i2.11304.
9. I. H. Midiana, "Analisis Yuridis Pengaturan Larangan Praktik Dark Patterns dalam E-Commerce di Indonesia (Studi Perbandingan Hukum Indonesia dengan Uni Eropa)," BSc Thesis, Universitas Brawijaya, 2024, Available: <http://repository.ub.ac.id/id/eprint/226675/1/Ivana%20Happy%20Midiana.pdf>
10. Autoriteit Consument & Markt (ACM), "UHT ACM over Uitvoeringswet digitale dienstenverordening," 2023, Available: <https://www.acm.nl/nl/publicaties/uht-acm-over-uitvoeringswet-digitaledienstenverordening>
11. P. M. Marzuki, "The Essence of Legal Research is to Resolve Legal Problems," *Yuridika*, vol. 37, no. 1, pp. 37–58, Mar. 2022, doi: 10.20473/ydk.v37i1.34597.
12. H. S. Zahratunnisa, I. Etiveni, B. Purwandari, and E. H. Purwaningsih, "How People Recognize Dark Pattern in E-Commerce?," *Journal of Information System*, vol. 21, no. 1, pp. 82–97, Mar. 2025, doi: 10.21609/jsi.v21i1.1479.
13. R. A. Pattiasina and S. M. D. Hutabarat, "Perlindungan Hukum terhadap Konsumen Grab Food Berdasarkan Ketidaksesuaian Informasi dalam Etiket Gambar," *Al Qalam*, vol. 17, no. 6, pp. 4105–4105, Nov. 2023, doi: 10.35931/aq.v17i6.2835.
14. R. R. Sabila Supardi and S. M. D. Hutabarat, "Comparative Legal Analysis of Indonesian and South Korean Consumer Protection in Cosmetic Safety Regulations," *Rechtsidee*, vol. 13, no. 1, Jun. 2025, doi: 10.21070/jihr.v13i1.1052.
15. N. A. Putih Merah and S. M. D. Hutabarat, "Perlindungan Hukum bagi Konsumen Marketplace terhadap Pencantuman Berat Bersih dalam Produk Makanan Kemasan," *Jurnal Cakrawala Hukum*, vol. 13, no. 1, pp. 58–67, Apr. 2022, doi: 10.26905/idjch.v13i1.5333.
16. Y. D. Novita and B. Santoso, "Urgensi Pembaharuan Regulasi Perlindungan Konsumen di Era Bisnis Digital," *Jurnal Pembangunan Hukum Indonesia*, vol. 3, no. 1, pp. 46–58, Jan. 2021, doi: 10.14710/jphi.v3i1.46-58.
17. G. Sylviana, D. P. Maharani, and A. M. Wibowo, "Keabsahan Praktik Dark Patterns terhadap Pemerolehan Persetujuan Pemrosesan Data Pribadi di Indonesia," *RechtJiva*, vol. 2, no. 1, pp. 66–85, Mar. 2025, doi: 10.21776/rechtjiva.v2n1.5.
18. European Parliament and Council of the European Union, "Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act)," *Official Journal of the European Union*, Oct. 2022, Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029>
19. European Parliament and Council of the European Union, "Directive 2005/29/EC concerning unfair business-to-consumer commercial practices," *Official Journal of the European Union*, Jun. 2005, Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029>
20. Autoriteit Consument & Markt (ACM), "ACM is now fully authorized to enforce the Digital Services Act," 2025, Available: <https://www.acm.nl/en/publications/acm-now-fully-authorized-enforce-digital-services-act>
21. Autoriteit Consument & Markt (ACM), "Leidraad Bescherming online consument," 2020, Available: <https://www.acm.nl/nl/publicaties/leidraad-bescherming-online-consument>
22. Autoriteit Consument & Markt (ACM), "ACM confronts online stores using misleading countdown timers," 2023, Available: <https://www.acm.nl/en/publications/acm-confronts-online-stores-using-misleading-countdown-timers-their-practices>
23. Autoriteit Consument & Markt (ACM), "ACM has fined online stores for using fake discounts," 2024, Available: <https://www.acm.nl/en/publications/acm-has-fined-online-stores-using-fake-discounts>
24. R. Armangau, "Consumer groups lodge complaint about Shein's online nudging with EU Commission," *Euronews*, 2025, Available: <https://www.euronews.com/next/2025/06/05/consumer-groups-lodge-complaint-about-sheins-online-nudging-with-eu-commission>
25. A. Earnshaw, "Digital Services Act: Shein becomes the latest VLOP to face formal proceedings," 2026, Available: <http://www.lewissilkin.com/insights/2026/02/27/digital-services-act-shein-becomes-the-latest-vlop-to-face-formal-proceedings-102mkps>
26. P. Arfanza and S. M. D. Hutabarat, "Perlindungan Konsumen atas Ketidaksesuaian Voucher Game Online pada Itemku," *NCOLS*, 2023, Available: <https://conference.upnvj.ac.id/index.php/ncols/article/view/2767>
27. H. Brono, "BPKN: Pengaduan Konsumen Meningkatkan, Negara Harus Hadir Lebih Tegas," *Koran Jakarta*, 2025, Available: <https://koran-jakarta.com/2025-12-16/bpkn-pengaduan-konsumen-meningkat-negara-harus-hadir-lebih-tegas>