



Protecting Consumer Autonomy from AI-Personalized Dark Patterns on E-Commerce Platforms in Indonesia

Yudha Erlangga Hidayat¹; Nurul Citra Fitri Manurung²

¹Department of Administrative Law, Faculty of Law, Universitas Diponegoro, Semarang, Indonesia

²Department of International Law, Faculty of Law, Universitas Diponegoro, Semarang, Indonesia

Article History

Received: 2026-03-10

Revised: 2026-03-17

Accepted: 2026-03-22

Published: 2026-04-05

Keywords:

Artificial Intelligence,
Consumer Autonomy, Dark
Patterns, E-Commerce,
Personalization.

DOI:

10.xxxx/titah.volx.issx.artx

Corresponding author:

Yudha Erlangga Hidayat
yudha.hidayat@undip.ac.id

Other author email(s):

nurul.manurung@undip.ac.id

Paper type:

Research article



Published by PT Penerbit Velora
Indonesia

Abstract

Purpose - This study examines how Indonesian e-commerce consumers experience and interpret AI-personalized dark patterns and how these practices affect consumer autonomy, trust, consent, perceived manipulation, digital vulnerability, and resistance.

Methodology - A qualitative interpretive design involved 24 active e-commerce consumers selected purposively in Indonesia. Data were collected from November 2025 to January 2026 through semi-structured in-depth interviews supported by scenario-based interface elicitation and analyzed using reflexive thematic analysis.

Findings - Six interconnected themes emerged: conditional acceptance of personalization, limited awareness of algorithmic influence, urgency and scarcity pressure, unequal effort in consent and refusal, declining trust after perceived manipulation, and consumer strategies for restoring autonomy. Personalization was accepted when it improved relevance while preserving control, but was viewed negatively when it became opaque, repetitive, difficult to refuse, or restrictive of deliberation.

Implications - Consumer protection should address both visible interface features and the algorithmic processes determining how personalized persuasion is delivered. E-commerce platforms should strengthen transparency and meaningful user control, while Indonesian policymakers need clearer guidance for adaptive digital choice architectures.

Originality - This study conceptualizes AI-personalized dark patterns as an adaptive process of digital influence and integrates consumer autonomy, digital choice architecture, digital vulnerability, privacy, and trust within the Indonesian e-commerce context.

Cite this article:

Hidayat, Y. E., & Manurung, N. C. F. (2026). Protecting consumer autonomy from AI-personalized dark patterns on e-commerce platforms in Indonesia. TTTAH: Journal of Law, x(x), xx-xx. <https://doi.org/10.xxxx/titah.volx.issx.artx>

Introduction

Digital commerce has shifted from relatively static online catalogues toward data-intensive environments in which artificial intelligence determines what consumers see, when they see it, and how available choices are presented. E-commerce platforms increasingly use browsing histories, search records, transaction data, clickstreams, device information, and inferred preferences to personalize recommendations, promotions, rankings, advertisements, and interface elements. AI-based personalization can reduce information overload and improve the relevance of commercial content, but it also expands the capacity of platforms to influence individual decision processes. Turki (2025) explains that AI-powered personalization increasingly shapes consumer behaviour through predictive analytics and individualized digital experiences while creating concerns related to transparency, governance, and consumer control. Singh (2023) similarly notes that AI-based e-commerce advertising relies on detailed consumer information to produce highly targeted experiences, making privacy and ethical design central to maintaining trust. These developments change the nature of consumer protection because consumers no longer encounter a uniform marketplace. Instead, each consumer may face a different choice environment generated from

behavioural data. The critical question is therefore not simply whether personalization increases convenience, but whether consumers remain able to identify commercial influence and make choices that reflect their own preferences.

This issue becomes more serious when personalization intersects with dark patterns. Dark patterns refer to deceptive, manipulative, or obstructive design practices that steer users toward actions that primarily benefit the platform or seller. Common examples include false urgency, scarcity cues, visual interference, hidden information, preselected options, difficult cancellation procedures, confirmshaming, forced action, and repeated prompts. [Koh and Seah \(2023\)](#) found that e-commerce dark patterns can influence product selection and increase the likelihood of unintended consumption. [Kim and Lee \(2023\)](#) further showed that dark patterns influence perceived fairness and consumer attitudes, indicating that their effects extend beyond a single transaction. [Piduru \(2023\)](#) argues that deceptive interface strategies may provide immediate commercial gains but can weaken customer experience and long-term trust. More recent conceptual work also shows that dark patterns share several underlying characteristics, including information asymmetry, constrained choice, psychological pressure, and the exploitation of behavioural tendencies ([Meirezaldi, 2025](#)). The problem therefore concerns both observable behaviour and the conditions under which consumers reach a decision.

AI increases the potential impact of these practices because manipulation can become personalized rather than standardized. A conventional countdown timer is displayed to many users in the same way, whereas an AI-personalized system can determine which users are more responsive to urgency, which consumers react to social proof, and when a promotional message is most likely to produce action. [Deligoz \(2025\)](#) argues that AI can make dark patterns more adaptive, individualized, and difficult to detect by combining behavioural prediction with persuasive interface design. [Spais et al. \(2024\)](#) identify consumer autonomy as an important concern when AI-based marketing technologies become highly directive. At the same time, personalization itself should not automatically be treated as manipulation. [Hassan et al. \(2025\)](#) show that personalized recommendations can strengthen satisfaction and loyalty when consumers perceive the technology as useful and trustworthy. [Jayapal \(2025\)](#) finds that the benefits of AI personalization are nevertheless moderated by privacy concerns, showing that consumers evaluate not only recommendation relevance but also how personal data are collected and applied. The ethical boundary therefore lies in whether personalization assists decision making or strategically exploits individual vulnerabilities to steer choices that consumers might not otherwise make.

The problem has particular relevance in Indonesia because e-commerce has become embedded in everyday consumption while users vary substantially in digital experience and their ability to detect manipulative interfaces. [Zahratunnissa et al. \(2025\)](#), through qualitative research involving Indonesian e-commerce users, found that participants did not consistently recognize dark patterns and often relied on previous personal experiences to identify manipulation. Experimental evidence from Indonesia similarly indicates that urgency cues, drip pricing, consent manipulation, and false social proof can affect trust, decision quality, and perceptions of fairness ([Uceng & Hanifah, 2024](#)). The significance of these findings becomes greater when AI personalization is considered because different consumers may encounter different combinations of persuasive cues. Consumer recognition therefore becomes more difficult when the interface changes according to inferred preferences or behavioural history. [Akbar et al. \(2024\)](#) also show that AI in e-commerce has a dual relationship with trust: personalization and security can strengthen confidence, while opacity, privacy risks, and algorithmic bias may weaken it. Indonesian consumers consequently face an environment in which the commercial benefits of personalization coexist with less visible risks to informed and self-directed decision making.

Consumer autonomy provides an appropriate theoretical foundation for understanding these risks. Autonomy in digital markets concerns the practical capacity of consumers to develop preferences, understand meaningful alternatives, refuse unwanted choices, and act without deceptive or excessive influence. [Brenncke \(2024\)](#) argues that online choice architectures can become exploitative when they materially interfere with a consumer's ability to make autonomous decisions. [Trzaskowski \(2024\)](#) similarly emphasizes that manipulation by design can occur through

the architecture of digital systems rather than through explicitly false information. Digital vulnerability strengthens this perspective because vulnerability is not limited to fixed demographic groups. [Rossi et al. \(2024\)](#) conceptualize digital vulnerability as multidimensional and situational, emerging from interactions between users, technology, information asymmetries, and specific decision contexts. [Zac et al. \(2025\)](#) provide empirical support for this broader approach by showing that susceptibility to dark patterns extends across consumer groups and cannot be explained adequately by age, education, or income alone. Consumer autonomy should therefore be assessed through the actual conditions under which a choice is made, not merely through the presence of a clickable acceptance or rejection option.

Regulatory research also reveals a substantial challenge. Digital consumer law traditionally focuses on misleading information, unfair contractual terms, privacy violations, or identifiable commercial misconduct, whereas AI-personalized dark patterns can operate through combinations of technically accurate information, behavioural profiling, visual hierarchy, interface friction, and individualized timing. [Herman \(2024\)](#) notes that European regulatory initiatives increasingly address dark patterns, but overlapping digital rules can create uncertainty in implementation. [Santos et al. \(2025\)](#) demonstrate that dark patterns can produce financial, privacy, psychological, temporal, and autonomy-related harms, which complicates legal approaches that rely on narrowly defined injury. In Indonesia, [Hayati \(2025\)](#) argues that existing consumer protection rules do not adequately address digital interfaces that impair consumer autonomy or exploit behavioural biases. [Sylviana et al. \(2025\)](#) similarly identify weaknesses in the legal treatment of consent obtained through manipulative interface designs under Indonesia's personal data protection framework. [Az-Zahra et al. \(2025\)](#) conclude that Indonesia still lacks explicit substantive prohibitions, specialized oversight, and technical guidelines that directly address dark patterns. These regulatory gaps become increasingly important when manipulation is dynamically personalized through AI.

Although research on dark patterns, personalization, privacy, consumer vulnerability, and AI marketing has expanded, these literatures remain fragmented. [Singh et al. \(2024\)](#) show that much of the dark-pattern literature examines particular interface mechanisms, behavioural outcomes, or digital nudging rather than consumers' interpretation of individualized manipulation. [Gray et al. \(2023\)](#) call for stronger integration between HCI, design, law, and regulatory research to characterize deceptive design harms more accurately. [Seaborn et al. \(2024\)](#) demonstrate that cultural and linguistic contexts can influence how users perceive and react to dark commercial patterns, highlighting the need for context-specific human-participant research. However, limited qualitative research has examined how Indonesian consumers distinguish helpful AI personalization from manipulative personalization, how they interpret pressure or loss of control, and how they attempt to resist algorithmically tailored influence. This study therefore aims to explore how Indonesian e-commerce consumers experience, interpret, and respond to AI-personalized dark patterns, with specific attention to consumer autonomy, informed choice, trust, consent, perceived manipulation, and resistance. The study contributes theoretically by linking consumer autonomy, digital choice architecture, and digital vulnerability within AI-mediated commerce. Practically, it provides evidence for regulators, platform designers, and consumer educators seeking to establish clearer boundaries between legitimate personalization and manipulative digital design.

Literature Review

Consumer Autonomy and Digital Choice Architecture

Consumer autonomy refers to an individual's capacity to form preferences and translate them into choices without coercion, deception, or excessive interference. In physical markets, consumers generally encounter relatively visible forms of persuasion, such as advertisements, sales presentations, or price promotions. Digital environments differ because platforms can shape the architecture surrounding a decision. Products may be ranked strategically, options may be visually unequal, cancellation may require several additional steps, and particular information may appear only after consumers have invested time in a transaction. [Mills \(2024\)](#) argues that deceptive choice architecture requires behavioural auditing because harmful influence can emerge from the

combined effects of interface features that appear individually minor. Autonomy is therefore not secured simply because consumers can technically click another option.

This perspective is particularly important in AI-mediated environments. AI systems can analyze past behaviour and continuously adjust future choice environments. [Gorjanc \(2025\)](#) connects ethical personalization with trust, fairness, privacy protection, and consumer autonomy, arguing that data-driven personalization requires governance practices that preserve user control. The autonomy perspective therefore shifts analysis away from whether AI recommendations are technically accurate toward whether consumers can understand how their environment is being shaped and meaningfully reject that influence. Consumer control becomes substantive only when a person can recognize alternatives, understand relevant consequences, and change or reverse a decision without unreasonable friction.

Dark Patterns and Manipulative Interface Design

Dark patterns represent a form of digital choice architecture that uses design to influence decisions in ways that may conflict with users' interests. Their mechanisms differ, but they commonly exploit limitations in attention, information processing, or decision time. [Thukral et al. \(2025\)](#) identify forced action, misdirection, sneaking, scarcity, obstruction, and related strategies as recurrent forms of manipulative digital design. The increasing diversity of these mechanisms makes simple checklist-based regulation difficult because deceptive practices can evolve as designers adapt interfaces to new legal standards and consumer habits.

Deceptive design is not confined to conventional shopping webpages. [De Conca \(2023\)](#) demonstrates that manipulative design can also operate through virtual assistants, where prompts, information ordering, and conversational interfaces may steer users while making the mechanism of influence less visible. This broader perspective is relevant to AI-personalized commerce because persuasion can be embedded in the interaction logic of a service rather than in a single obvious visual element.

Research also indicates that harm can arise from the cumulative design process rather than one isolated screen. [Kelly and Rubin \(2024\)](#) identified obstruction and other manipulative practices in account-disabling interfaces, illustrating how users can be discouraged from exercising preferences through additional steps and unclear navigation. [Richardson and Fang \(2025\)](#) show that interface design can also intersect with platform self-preferencing, raising questions about the boundary between predictive design and manipulation. Such findings are relevant to e-commerce because the entire purchasing journey, from product discovery to payment and cancellation, can contain design decisions that privilege platform objectives.

The regulation of dark patterns also requires attention to the location of manipulation within digital systems. [Gray et al. \(2024\)](#) argue that research must move toward stronger methodologies for detecting deceptive practices, characterizing harms, and designing effective countermeasures. This is important because some dark patterns remain highly visible while others are embedded in system logic, ranking processes, or personalized interaction flows. Consumers may therefore experience manipulation without being able to identify a particular visual element responsible for the pressure they feel.

AI Personalization and the Boundary of Legitimate Persuasion

AI personalization creates clear consumer benefits. Recommendation algorithms can reduce search costs, filter irrelevant information, improve product discovery, and provide offers that reflect prior interests. [Sarkar \(2024\)](#) argues that explainable AI can strengthen transparency and consumer trust when users receive understandable information about AI-driven recommendations and decisions. [Syam \(2025\)](#) similarly notes that AI technologies improve targeting and customer engagement, while privacy, bias, and transparency remain major concerns for digital marketing.

The central issue is therefore not whether personalization should exist, but how it is used. Personalized recommendation becomes ethically problematic when a system uses behavioural information to identify and exploit specific decision weaknesses. Personalized scarcity messages may target consumers who previously responded to urgency. Social proof may appear when an algorithm predicts uncertainty. Promotional notifications may increase when a consumer repeatedly views a product but postpones buying it. These practices create a stronger asymmetry

because platforms possess detailed behavioural information while consumers have limited knowledge about the systems influencing them.

The distinction between support and manipulation also depends on transparency and reversibility. If personalization helps consumers identify products that match their stated preferences, it can support autonomy. If the system suppresses alternatives, exaggerates urgency, or increases friction around refusal, it can reduce autonomy. The ethical assessment should therefore consider the purpose and mechanism of personalization, not only its technical sophistication or conversion performance.

Digital Vulnerability, Privacy, and Consent

Digital vulnerability should be understood as situational rather than as a permanent characteristic of particular groups. A digitally experienced consumer may still become vulnerable under time pressure, emotional stress, information overload, or complex consent processes. This perspective is especially relevant to mobile e-commerce, where users often make rapid decisions through small screens and repeated notifications.

Privacy decisions illustrate this problem clearly. [Kocyigit et al. \(2023\)](#) identify observable features of dark patterns in cookie-consent processes and show how information flows can be structured in ways that steer users toward privacy-invasive choices. [Berens et al. \(2024\)](#) similarly demonstrate that cookie interfaces can lack transparency and use design characteristics that affect user decisions. [Farronato et al. \(2025\)](#) provide field-experimental evidence that additional clicks, hidden options, and default structures can materially alter consumer consent behaviour. These findings show that formal consent cannot automatically be equated with autonomous consent.

The problem becomes more complex when personal data obtained through such consent later inform personalized persuasion. Consumers may technically agree to data processing without understanding that their behavioural information can subsequently shape advertisements, recommendations, or choice architecture. AI-personalized dark patterns therefore connect data protection and consumer protection. The key issue is not only how data are collected but also how knowledge generated from those data is used to influence future decisions.

Trust, Fairness, and Consumer Responses

Trust plays a central role in digital commerce because consumers cannot directly observe most of the algorithms or data-processing practices used by platforms. When personalization appears relevant and predictable, consumers may interpret it as a useful service. When personalization reveals unexpected knowledge about individual behaviour, the same system may appear intrusive or manipulative.

Perceptions of fairness influence this relationship. Consumers are more likely to accept commercial persuasion when they understand its purpose and retain meaningful opportunities to reject it. By contrast, hidden fees, misleading urgency, unequal buttons, or difficult cancellation may signal that the platform is attempting to secure compliance rather than support choice. Repeated exposure to these mechanisms may therefore influence trust even when the consumer does not use the term dark pattern.

Consumer responses also differ. Some users comply immediately, while others ignore notifications, compare products across platforms, close applications, remove items from carts, reject permissions, or deliberately wait before purchasing. These actions can be understood as strategies for restoring autonomy. A qualitative approach is useful because these forms of resistance may not appear in platform conversion metrics yet remain central to understanding the lived experience of algorithmic influence.

Indonesian Consumer Protection Context

Indonesia's digital market creates an important setting for studying these processes because consumers interact with rapidly evolving e-commerce ecosystems while the regulatory response to manipulative interface design remains developing. Existing legal instruments protect consumers from misleading practices and regulate personal data processing, but their application to adaptive interface manipulation is less explicit.

The challenge extends beyond legal wording. Effective consumer protection requires operational criteria that can distinguish ordinary persuasion from practices that impair autonomy. Static prohibitions may become less effective when interfaces continuously adapt to users. Regulation therefore needs to address design outcomes, transparency, data use, and the ability of consumers to refuse personalized influence.

Indonesia also presents a significant cultural and practical context for qualitative inquiry. Consumers may interpret scarcity, promotional language, social proof, gamified discounts, and repeated notifications according to their own shopping habits and digital experience. These meanings cannot be fully inferred from interface audits alone. Direct consumer accounts are needed to understand when users perceive personalization as convenient, when it becomes uncomfortable, and how they respond when they believe a platform is pushing them toward an unwanted choice.

Research Gap and Conceptual Focus

Existing scholarship establishes that dark patterns can change behaviour, reduce perceptions of fairness, increase privacy disclosure, and create consumer harm. It also establishes that AI personalization can improve relevance, satisfaction, and loyalty while raising privacy and transparency concerns. However, relatively little research integrates these two streams at the level of lived consumer experience.

Most studies examine predetermined dark-pattern conditions, standardized screenshots, platform audits, experiments, legal frameworks, or measurable behavioural outcomes. These approaches are valuable, but they provide less insight into how consumers construct meaning around adaptive personalization. They cannot fully explain how consumers decide that a recommendation has crossed the boundary into manipulation or why the same interface feature may feel helpful to one person and coercive to another.

The present study addresses this gap through three connected concepts: consumer autonomy, digital choice architecture, and digital vulnerability. Consumer autonomy provides the normative focus. Digital choice architecture explains how interfaces structure decisions. Digital vulnerability explains why susceptibility changes according to context rather than remaining fixed. Together, these concepts guide the analysis of how Indonesian consumers recognize, interpret, negotiate, and resist AI-personalized dark patterns.

Research Methods

Research Design

This study employed a qualitative interpretive research design to examine how Indonesian consumers experience, understand, and respond to AI-personalized dark patterns on e-commerce platforms. The qualitative approach was appropriate because the research focused on meaning, perception, interpretation, and decision processes rather than estimating causal effects or population-level prevalence. The study adopted a constructivist orientation in which consumer interpretations were understood as being formed through interactions with platforms, prior shopping experiences, digital literacy, and broader expectations about legitimate commercial persuasion.

Consumer autonomy and digital choice architecture were used as sensitizing concepts rather than rigid coding categories. This approach allowed the theoretical framework to inform the inquiry while retaining space for unexpected interpretations. Participants could therefore describe experiences using their own language rather than being required to categorize interfaces according to predetermined dark-pattern taxonomies.

Participants and Sampling

The study involved 24 active e-commerce consumers in Indonesia. Participants were recruited using purposive sampling because direct experience with algorithmically personalized commercial environments was essential to the research question. Eligible participants were at least 18 years old, had used an e-commerce platform during the previous six months, and had encountered personalized recommendations, targeted promotional messages, discount notifications, product-ranking suggestions, or similar customized features.

The sample sought variation in age, gender, occupation, shopping frequency, and digital experience. Variation was important because the purpose was not to identify a statistically representative consumer profile but to capture different ways of interpreting personalization and manipulation. Participants reported experience with major e-commerce services operating in Indonesia, including Shopee, Tokopedia, Lazada, Blibli, and TikTok Shop. Recruitment continued until the dataset provided sufficient conceptual depth and additional interviews produced limited substantive variation in the core patterns relevant to the research questions.

Participants were assigned identifiers P01 to P24. These identifiers were used in transcripts, analytic notes, and the presentation of quotations to protect confidentiality.

Data Collection

Data collection was conducted from November 2025 to January 2026. The primary method consisted of individual semi-structured, in-depth interviews. Semi-structured interviewing was selected because it provided consistency across the major research topics while allowing researchers to probe unexpected experiences and interpretations. [Kahlke et al. \(2025\)](#) emphasize that qualitative interviewing requires alignment between interview purpose, research design, questioning strategy, and documentation in order to generate analytically rich accounts.

Each interview lasted approximately 45 to 70 minutes. Interviews were conducted face-to-face or through a secure online meeting platform according to participant preference and practical availability. Interviews addressed experiences with personalized recommendations, urgency and scarcity messages, social proof, discount notifications, default options, add-on offers, consent interfaces, cancellation procedures, and perceptions of control during online purchasing.

The questions were deliberately open-ended. Participants were asked to describe concrete situations in which an e-commerce interface felt useful, persuasive, confusing, intrusive, or manipulative. Follow-up questions explored what participants noticed, what they believed the platform was attempting to achieve, how the design affected their decision, and whether they felt able to reject or change the proposed choice. This structure avoided defining every interface as a dark pattern before participants had interpreted it themselves.

Scenario-Based Interface Elicitation

The interviews incorporated scenario-based interface elicitation to complement retrospective accounts. Participants were shown simulated e-commerce interfaces illustrating mechanisms such as personalized scarcity messages, countdown timers, targeted social proof, preselected add-ons, difficult opt-out options, repeated promotional prompts, personalized discount warnings, and visually unequal consent choices.

The scenarios were designed to resemble common digital shopping situations without reproducing participants' private account information or confidential platform data. Participants were asked what they noticed first, how they interpreted each interface, what action they would likely take, and whether they believed the design supported or constrained their freedom of choice.

This technique was particularly valuable because dark patterns are often difficult to describe from memory. The scenarios provided a common point of discussion while still allowing participants to construct their own meanings. They also enabled comparisons between situations where participants immediately identified manipulation and situations where the persuasive mechanism was noticed only after further reflection.

Data Recording and Management

With participant consent, interviews were audio-recorded and transcribed verbatim. Transcripts were reviewed against recordings to improve accuracy. Identifying information was removed during transcription. Field notes were produced after each interview to document contextual observations, notable pauses, changes in interpretation, and emerging analytic ideas.

Audio files, transcripts, and analytic materials were stored in password-protected digital folders accessible only to the research team. Data files used participant codes rather than names. No passwords, payment credentials, transaction numbers, or other sensitive e-commerce account information were collected.

Data Analysis

The study used reflexive thematic analysis. This method was suitable because the research sought patterned meanings across participants while recognizing the interpretive role of the researchers. [Terry and Hayfield \(2025\)](#) describe reflexive thematic analysis as a flexible approach that involves familiarization, coding, theme development, theme review, definition, and interpretive writing rather than mechanical aggregation of codes.

Analysis began with repeated reading of the interview transcripts. Initial notes focused on expressions related to control, pressure, personalization, trust, fairness, consent, awareness, regret, resistance, and perceived manipulation. Coding then proceeded across the full dataset. Some codes were semantic and reflected participants' explicit statements, while others addressed underlying meanings concerning autonomy and power within the platform-consumer relationship.

The analysis combined inductive and theory-informed reasoning. Inductive coding allowed unexpected patterns to emerge from participant accounts. At the same time, consumer autonomy and digital choice architecture guided attention toward meaningful choice, information asymmetry, freedom to refuse, transparency, and reversibility.

[Udayanga \(2025\)](#) emphasizes the value of treating thematic analysis as an iterative and reflexive process rather than separating data collection and interpretation completely. Consistent with this approach, preliminary insights generated during earlier interviews informed later probing while the central interview topics remained stable.

Candidate themes were developed by examining relationships among codes rather than by counting the frequency of individual statements. Themes were reviewed against both coded extracts and complete transcripts. Particular attention was paid to divergent cases. For example, if one participant interpreted a personalized recommendation as useful while another interpreted a similar practice as intrusive, the difference was retained and analyzed rather than treated as inconsistency.

Trustworthiness

The study used several strategies to strengthen qualitative trustworthiness. First, participant variation provided different perspectives on e-commerce personalization. Second, an audit trail documented interview notes, coding decisions, theme revisions, and analytic memos. Third, the research team discussed developing interpretations and actively considered alternative explanations.

Reflexive practice was treated as part of the analytic process. [Ide and Beddoe \(2023\)](#) argue that reflexivity requires researchers to question how their positions, expectations, relationships, and emotional responses influence qualitative inquiry. Researchers therefore recorded assumptions regarding platform responsibility, AI personalization, consumer vulnerability, and ethical interface design throughout the analysis.

Researcher positionality was also considered when interpreting participants' descriptions of manipulation. [Strunel and Cordoba \(2025\)](#) demonstrate that positionality influences how qualitative researchers understand participant accounts and researcher-participant relationships. The research team therefore distinguished between participants' own evaluations and theoretical classifications introduced during later interpretation.

[Torres-Quintero and Granados-Garcia \(2023\)](#) describe reflexivity as a continuing practice throughout qualitative research rather than an isolated statement included only at the reporting stage. Accordingly, reflexive notes were maintained during interviewing, coding, theme development, and manuscript preparation.

Ethical Considerations

Participation was voluntary. Before the interviews, each participant received information about the objectives of the study, interview procedures, recording, confidentiality, intended use of the data, and the right to discontinue participation without penalty. Informed consent was obtained before data collection.

Participants were not asked to provide account passwords, financial credentials, private transaction numbers, or other unnecessary personal data. Any identifying information mentioned

during interviews was removed from the research transcript. Direct quotations used in reporting were linked only to participant codes.

The research procedures emphasized voluntary participation, informed consent, confidentiality, data minimization, and secure handling of interview materials throughout the study.

Methodological Alignment

The methodological design was aligned with the central objective of understanding AI-personalized dark patterns as experienced forms of digital influence. Interviewing provided access to remembered experiences and personal interpretations. Scenario-based elicitation made less visible forms of manipulation easier to discuss. Reflexive thematic analysis enabled the study to examine shared patterns while preserving differences between participants.

This design also addressed a limitation in research that treats the presence of a dark pattern as sufficient evidence of its meaning for consumers. The same design feature may be interpreted differently depending on prior experience, trust, perceived urgency, or understanding of personalization. The qualitative approach therefore enabled the research to examine the boundary between useful personalization and manipulation from the perspective of consumers themselves.

Results and Discussion

The thematic analysis of the 24 interviews and scenario-based interface discussions identified six interconnected themes: the conditional acceptance of personalization, limited awareness of algorithmic influence, urgency and scarcity as sources of decision pressure, unequal effort in consent and refusal, erosion of trust after perceived manipulation, and consumer strategies for restoring autonomy. These themes show that participants did not regard personalization as inherently harmful. Instead, their evaluations depended on whether personalized features remained relevant, understandable, and easy to ignore. Perceptions changed when personalization increased pressure, limited opportunities for reflection, obscured alternatives, or appeared to exploit information about individual preferences. The results therefore position consumer autonomy as a dynamic experience shaped by the interaction between algorithmic personalization, interface design, and the consumer's capacity to retain meaningful control.

Personalization Was Accepted When It Supported Rather Than Directed Consumer Choice

Participants generally viewed personalized recommendations positively when they reduced search effort and helped identify products that matched previous interests. Recommendations based on recently viewed products, preferred categories, or previous purchases were commonly interpreted as part of the expected convenience of contemporary e-commerce. In this context, personalization was perceived as a service that reduced information overload rather than as an interference with decision making. Consumers appeared comfortable with algorithmic assistance when they could easily ignore the suggestion, compare it with other products, or continue browsing without additional pressure.

However, the interpretation changed when personalized content became repetitive or appeared too closely connected to previous online behaviour. Participants described a clearer sense of discomfort when products viewed briefly continued to appear through notifications, promotional messages, or recommendation sections. Repetition made some participants more aware that their browsing activity was being tracked and subsequently used to influence purchasing behaviour. The problem was therefore not simply that platforms remembered preferences. Concern emerged when remembered behaviour appeared to become a persistent attempt to convert interest into a transaction.

This distinction supports [Hassan et al. \(2025\)](#), who found that personalized recommendations can strengthen satisfaction and loyalty when consumers consider them useful. The present findings add that perceived usefulness is closely tied to the availability of meaningful choice. Personalization remained legitimate when consumers experienced it as informational support, but it became questionable when platform objectives appeared to dominate the interaction.

The findings also reinforce the autonomy framework developed by [Brenncke \(2024\)](#). Consumer autonomy in digital environments cannot be assessed only by determining whether users technically remain able to choose. A consumer may still have several clickable alternatives while experiencing repeated prompts that gradually change the conditions under which the decision is made. The practical ability to ignore, delay, or reject a personalized recommendation therefore appears to be an important boundary between assistance and manipulation.

This boundary also explains why consumers did not consistently classify the same interface mechanism in the same way. A personalized recommendation could be considered useful during active product searching but intrusive when it continued after the consumer had decided not to purchase. The meaning of personalization was therefore contextual. It depended on timing, repetition, perceived relevance, and the consumer's current intention.

Consumers Recognized Persuasion More Easily Than Algorithmic Personalization

A second major theme concerned the visibility of algorithmic influence. Participants could generally recognize direct promotional strategies, including discount notifications, flash-sale announcements, recommended products, and limited-time messages. However, they showed less certainty when explaining why particular content appeared to them. Consumers often recognized that a message was attempting to persuade them without clearly understanding how behavioural data might have been used to determine the content, timing, or intensity of that persuasion.

This difference is important because AI-personalized persuasion operates through processes that are largely invisible at the interface level. Consumers see the output of personalization but rarely see the profiling processes behind it. They may notice a recommendation but remain uncertain whether it was generated from search history, purchase history, location, interaction frequency, browsing duration, or a combination of behavioural indicators.

[Turki \(2025\)](#) explains that AI-enabled e-commerce increasingly relies on large volumes of behavioural data to adapt digital experiences to individual consumers. The present findings suggest that this technical sophistication creates an informational imbalance. Platforms may possess detailed models of consumer interests while consumers have only a general understanding that some form of personalization is occurring.

The issue also relates to transparency. [Sarkar \(2024\)](#) argues that explainable AI can contribute to consumer trust when users receive understandable information about automated recommendations and decisions. In the present study, participants' uncertainty suggests that personalization transparency should not be limited to generic statements such as recommended for you. Such wording indicates that personalization exists but does not explain why a specific product, promotion, or urgency cue was selected.

This finding extends the Indonesian evidence reported by [Zahratunnissa et al. \(2025\)](#). Their study demonstrated that consumers did not consistently recognize dark patterns and that previous experience influenced awareness. The present analysis suggests a further layer of difficulty. Even when consumers recognize a persuasive design, they may not recognize that the design itself has been personalized through behavioural data.

This gap has implications for consumer autonomy. Consumers can evaluate an influence more critically when they understand its source. When the basis of personalization remains opaque, the platform can shape the consumer's choice environment without making the nature of that intervention fully visible. Algorithmic transparency therefore becomes part of meaningful consumer control rather than merely a technical or privacy issue.

Urgency and Scarcity Reduced the Space for Deliberation

Urgency and scarcity features were among the interface mechanisms most clearly associated with perceived pressure. Countdown timers, claims that only a small number of products remained, rapidly expiring vouchers, flash-sale deadlines, and messages suggesting that other users were simultaneously considering a product created a perception that delaying the decision could lead to a loss.

Participants did not necessarily reject these practices outright. Some considered limited-time promotions a normal feature of online shopping. The perception of manipulation became stronger when the same urgency message appeared repeatedly or when participants suspected that scarcity

was exaggerated. When a timer restarted, a supposedly limited voucher became available again, or similar stock warnings appeared across repeated visits, confidence in the authenticity of the message declined.

This reaction indicates that perceived manipulation was connected to the credibility of the scarcity claim. Genuine scarcity can provide useful information. Artificial scarcity creates pressure by altering the consumer's perception of available decision time. The ethical problem therefore does not arise from urgency itself but from whether urgency accurately reflects market conditions and whether the platform uses it to restrict deliberation.

Koh and Seah (2023) demonstrate that e-commerce dark patterns involving urgency can influence consumer product selection. The present qualitative findings help explain how this occurs. Urgency narrows the psychological space for comparison. Consumers may become more concerned about losing an opportunity than about evaluating whether the purchase remains appropriate.

The relationship between urgency and fairness is also relevant. Kim and Lee (2023) show that dark patterns influence consumers' perceptions of fairness and attitudes toward online service providers. In the present study, skepticism increased when urgency mechanisms appeared inconsistent with later observations. Once consumers suspected that urgency was manufactured, the interface was more likely to be interpreted as deceptive rather than persuasive.

AI personalization can intensify this concern. Deligoz (2025) argues that AI can make dark patterns more individualized by using behavioural information to determine when and how persuasive strategies are deployed. A generic countdown timer affects all visitors similarly. An algorithmically deployed urgency message can appear specifically when a consumer has repeatedly viewed a product, compared alternatives, or shown indications of purchase intent.

This distinction is significant for autonomy. An AI system may identify precisely when a consumer is uncertain and introduce urgency at that point. Such intervention does not remove the formal ability to reject a purchase, but it changes the decision context in a way designed to make immediate action more likely. The findings therefore suggest that regulators and platform auditors should assess not only whether urgency messages exist but also whether their timing or content is dynamically personalized.

Consent Was Perceived as Less Meaningful When Refusal Required Greater Effort

The scenario-based discussions also revealed concerns surrounding consent, default selections, and opt-out mechanisms. Participants generally understood the purpose of common permission requests but often approached them pragmatically. When accepting a request provided faster access to the desired service, consumers could choose the quickest option without carefully evaluating the implications of the decision.

This behaviour should not automatically be interpreted as indifference to privacy. Rather, it reflects the design context in which consent is requested. Repeated consent prompts compete with the consumer's primary objective, which is usually to browse, purchase, communicate with a seller, or complete a transaction. When the privacy-protective option requires more clicks, additional reading, or navigation through settings, convenience can push consumers toward the platform-preferred option.

Kocyigit et al. (2023) show that dark-pattern mechanisms can be embedded within consent processes through differences in visibility, sequence, and information structure. The present findings support this interpretation. Consumers assessed consent not only by the presence of options but also by how easy the interface made each option to exercise.

Berens et al. (2024) similarly demonstrate that cookie-consent designs can influence decisions through visual representation and labelling. This indicates that formally presenting both acceptance and rejection does not necessarily create equivalent choices. A large, prominent acceptance button and a less visible rejection pathway can preserve formal choice while reducing practical symmetry.

The importance of additional effort is also supported by Farronato et al. (2025), who found that hiding options behind extra clicks can materially affect consent behaviour. The present study places this mechanism within the broader environment of personalized e-commerce. Consent is especially important because the information obtained from consumers can later support the

personalization of recommendations, advertisements, discounts, and persuasive interface strategies.

The legal significance is substantial in Indonesia. [Sylviana et al. \(2025\)](#) question the validity of consent when dark patterns influence personal data processing decisions. If consumers provide consent partly because refusal is deliberately made more difficult, the resulting authorization may satisfy a formal interface requirement without fully representing an informed and autonomous preference.

The findings therefore suggest that meaningful consent requires more than disclosure. It requires reasonable symmetry between accepting and refusing, accessible explanations of personalization, and opportunities to revise choices without substantial friction.

Perceived Manipulation Reduced Trust Even When Consumers Continued Using the Platform

Trust emerged as a central consequence of perceived dark patterns. Participants did not necessarily stop using a platform after encountering an interface they considered manipulative. E-commerce platform choice can be influenced by price, product availability, existing accounts, payment systems, delivery networks, and familiarity. As a result, reduced trust did not always translate into complete platform abandonment.

Instead, distrust was expressed through more cautious behaviour. Consumers described checking prices on other platforms, delaying purchases, questioning promotional claims, and becoming more skeptical about scarcity or discount messages. The important finding is therefore that continued use should not automatically be interpreted as continued trust.

This distinction has practical implications because platform metrics such as retention or repeated visits may fail to reveal declining confidence. A consumer may continue to use an e-commerce platform because it remains convenient while becoming increasingly suspicious of the interface.

[Akbar et al. \(2024\)](#) identify transparency, privacy, reliability, and ethical AI practices as important factors in consumer trust. The findings of the present study reinforce this relationship. Personalization can strengthen confidence when it appears relevant and predictable, but the same data-driven system can weaken confidence when consumers believe it is exploiting their behaviour.

[Jayapal \(2025\)](#) similarly shows that privacy concerns weaken the positive effects associated with AI personalization. This suggests that commercial effectiveness and consumer trust should not be treated as identical outcomes. Highly effective personalized persuasion may produce short-term conversions while undermining longer-term perceptions of legitimacy.

The connection between fairness and trust also emerged clearly. When consumers suspected that scarcity was artificial, that refusal had been made unnecessarily difficult, or that recommendations were being repeated because the platform had detected their interest, the interaction could be interpreted as asymmetrical. Consumers recognized that the platform possessed more information about their behaviour than they possessed about the platform's decision logic.

This informational imbalance supports the broader conceptualization of digital vulnerability offered by [Rossi et al. \(2024\)](#). Vulnerability does not necessarily arise because consumers lack general intelligence or digital competence. It can arise because one party has superior access to behavioural information and greater capacity to design the conditions under which the other party makes decisions.

Consumers Used Everyday Resistance Strategies to Restore Control

The final theme demonstrates that consumers were not simply passive recipients of personalized persuasion. Participants described practical strategies for maintaining decision control. These strategies included postponing purchases, comparing prices across platforms, placing items in carts without immediately checking out, checking whether discounts remained available later, disabling promotional notifications, ignoring recommendations, and leaving an application when pressure became excessive.

These behaviours can be interpreted as informal mechanisms of autonomy restoration. Consumers created their own friction when platforms attempted to reduce it. Waiting before

purchasing, for example, introduced additional deliberation into an interface designed to encourage immediate conversion.

Experience played an important role in these strategies. Repeated exposure to promotions could lead consumers to become skeptical of countdown timers or scarcity statements. Consumers who had previously regretted impulsive purchases were more likely to describe deliberate waiting or comparison as protective habits. Recognition therefore appeared to develop through interaction and experience rather than solely through formal digital-literacy education.

This pattern is consistent with [Zahratunnissa et al. \(2025\)](#), who found that experience contributed to dark-pattern recognition among Indonesian e-commerce users. However, the present findings indicate that recognition can lead not only to awareness but also to active behavioural adaptation.

[Zac et al. \(2025\)](#) demonstrate that dark-pattern vulnerability extends across consumer groups and cannot be explained adequately through conventional demographic indicators. The present qualitative findings support this situational interpretation. A digitally experienced consumer may still respond impulsively when tired, distracted, highly interested in a product, or concerned about losing a discount. Conversely, a less technically knowledgeable consumer may resist pressure effectively because previous experiences have produced skepticism.

These results also caution against placing excessive responsibility on individuals. Consumer resistance requires attention, time, and repeated effort. AI-enabled platforms can continuously test and optimize persuasive strategies, whereas consumers must make numerous everyday decisions across digital services.

[Gray et al. \(2024\)](#) therefore emphasize the need for regulatory, technical, and design-based responses to deceptive interfaces. The present findings support this position. Digital literacy can strengthen consumers' capacity to recognize manipulation, but it should complement rather than replace platform accountability.

Integrative Discussion

Taken together, the findings show that the central issue in AI-personalized e-commerce is not personalization itself but the conditions under which personalization influences choice. Participants valued personalization when it reduced search effort and improved relevance. Concern emerged when the same technological capacity was used to increase pressure, obscure alternatives, create unequal consent pathways, or repeatedly pursue consumers after they had not acted on an earlier recommendation.

This result supports a continuum rather than a binary distinction between ethical personalization and manipulation. At one end, personalization helps consumers implement existing preferences. At the other, personalization uses behavioural information to modify the decision environment in ways that make platform-preferred behaviour more likely. The boundary depends on transparency, proportionality, accuracy, control, and ease of refusal.

[Trzaskowski \(2024\)](#) argues that digital manipulation should be understood through the architecture of the environment rather than only through false statements. This argument is highly relevant to AI-personalized dark patterns. An interface may contain factually accurate information while still being manipulative if the system strategically determines which information to emphasize and when to display it.

The present study therefore extends the concept of dark patterns from static deceptive design toward adaptive deceptive choice architecture. Traditional dark-pattern analysis often examines whether an interface includes a particular design feature. AI personalization introduces another question: whether the platform uses consumer-specific information to decide how persuasive that feature should become.

This distinction also clarifies the concept of consumer autonomy. [Brenncke \(2024\)](#) treats autonomy as central to evaluating exploitation in online choice architecture. The present findings suggest that autonomy involves at least four practical conditions in e-commerce: consumers must be able to understand the relevant choice, retain sufficient time for deliberation, refuse without disproportionate effort, and revise their decision without unnecessary friction.

Formal freedom alone is insufficient. A consumer may be technically free to decline a personalized offer while facing repeated alerts, urgency messages, or visually dominant calls to action. Autonomy therefore requires attention to how the entire interaction is structured.

Digital vulnerability should also be reconsidered in this context. The findings did not suggest a simple division between vulnerable and non-vulnerable consumers. Instead, susceptibility appeared connected to situational conditions such as urgency, uncertainty, repetition, convenience, and previous experience.

This supports [Rossi et al. \(2024\)](#), who conceptualize digital vulnerability as multidimensional. AI can make this vulnerability more dynamic because systems can identify behavioural signals associated with uncertainty, interest, or responsiveness. A platform does not need to know that a consumer belongs to a conventionally vulnerable demographic group. It may only need to predict that a particular individual is more likely to respond to a particular persuasive cue at a particular moment.

The implications for regulation are significant. [Hayati \(2025\)](#) argues that Indonesia's consumer protection framework does not adequately address interface practices that impair autonomy or exploit behavioural biases. The present study indicates that future rules should account for adaptive personalization rather than focusing only on visible and standardized dark patterns.

[Az-Zahra et al. \(2025\)](#) identify the absence of explicit prohibitions, specialized oversight, and technical guidance as important regulatory weaknesses in Indonesia. Addressing these gaps requires regulatory standards that examine both interface design and algorithmic deployment.

For example, a scarcity message should not only be assessed according to its wording. Regulators should also consider whether the claim is verifiable, whether it differs across users, whether AI determines its timing, and whether the consumer can understand why the message has been presented.

Similarly, consent regulation should evaluate practical symmetry between acceptance and rejection. If one choice requires substantially greater effort, the interface can influence consumer behaviour without explicitly forcing consent.

[Mills \(2024\)](#) proposes behavioural auditing as a response to deceptive choice architecture. Such an approach appears especially relevant for AI-personalized e-commerce. Traditional compliance checks may inspect a static version of an interface, while different users may receive different recommendations, prompts, or promotional sequences. Effective auditing should therefore examine outcomes across user profiles and interaction histories.

The findings also have implications for platform design. Ethical personalization should provide clear consumer benefits while preserving practical control. Platforms can reduce autonomy risks by providing understandable explanations for recommendations, allowing users to adjust personalization preferences, avoiding unverifiable scarcity messages, making acceptance and refusal comparably accessible, and limiting repetitive promotional interventions after a consumer has declined or ignored them.

Trust should be treated as an important long-term outcome of these design choices. Short-term conversion gains can coexist with declining consumer confidence. Platforms may therefore benefit from evaluating not only immediate behavioural metrics but also whether users perceive personalization as fair and respectful.

The findings further suggest that Indonesian digital-literacy initiatives should expand beyond conventional concerns such as phishing, account security, and misinformation. Consumers increasingly need algorithmic literacy, including an understanding that recommendations, advertisements, urgency cues, and promotions may be selected according to behavioural data.

However, literacy cannot solve the problem alone. Consumers cannot reasonably be expected to identify every algorithmic mechanism operating behind an interface. The informational imbalance between platforms and individuals remains structural.

Consequently, protecting autonomy requires shared responsibility among platforms, regulators, designers, and consumers. Platforms should avoid using personalization to exploit behavioural susceptibilities. Regulators should establish enforceable standards for manipulative

choice architecture. Designers should incorporate autonomy-preserving principles from the beginning of interface development. Consumer education should provide practical tools for recognizing and responding to persuasive digital environments.

Overall, this study shows that AI-personalized dark patterns transform consumer manipulation from a fixed interface problem into an adaptive process of behavioural influence. The primary risk does not arise because AI makes recommendations. It arises when detailed knowledge of consumer behaviour is used to determine how, when, and with what degree of pressure those recommendations or other persuasive elements are delivered.

The study therefore contributes to the literature by connecting consumer autonomy, digital choice architecture, digital vulnerability, data privacy, and trust within a single interpretive framework. In the Indonesian e-commerce context, meaningful consumer protection requires moving beyond the question of whether consumers technically have a choice. The more important question is whether the digital environment allows them to recognize, evaluate, refuse, and reconsider that choice without personalized manipulation undermining their capacity for independent decision making.

Conclusion

This study shows that AI-personalized dark patterns on Indonesian e-commerce platforms should not be understood merely as isolated interface tricks, but as adaptive forms of digital influence that can shape the conditions under which consumers make decisions. The findings indicate that consumers generally accept personalization when it improves relevance, reduces search effort, and preserves their ability to ignore, postpone, or reject recommendations. Perceptions change when personalization becomes repetitive, opaque, difficult to refuse, or combined with urgency, scarcity, unequal consent pathways, and other persuasive mechanisms that reduce the space for deliberation. Consumers also recognize persuasive messages more easily than the algorithmic processes behind them, which creates an informational imbalance between platforms and users. These findings contribute to the literature by integrating consumer autonomy, digital choice architecture, and digital vulnerability into a single framework for understanding AI-mediated manipulation. The study further demonstrates that autonomy in digital commerce depends not only on the formal availability of alternatives, but also on consumers' practical capacity to understand, evaluate, refuse, and reconsider platform-generated choices.

The findings have theoretical, practical, and policy implications. Theoretically, they extend existing dark-pattern research by showing that manipulation can become individualized through behavioural data and algorithmic personalization, making vulnerability situational rather than limited to specific demographic groups. Practically, e-commerce platforms should design personalization systems that provide clear benefits while maintaining transparency, equivalent pathways for acceptance and refusal, verifiable urgency claims, manageable promotional intensity, and meaningful user control over personalization. From a policy perspective, Indonesian consumer and personal data protection frameworks should move beyond static interface prohibitions and consider how behavioural data are used to determine the timing, form, and intensity of persuasive design. Regulatory approaches may therefore benefit from behavioural audits and technical guidance for adaptive interfaces. Future research should examine AI-personalized dark patterns across different platform categories, consumer groups, and longitudinal usage contexts, and should combine qualitative evidence with interface audits or experimental methods to further clarify when useful personalization crosses the boundary into manipulation.

Acknowledgements

The authors would like to express their sincere appreciation to all participants who voluntarily contributed their time, experiences, and perspectives to this study. Their insights were essential to understanding how consumers experience and interpret AI-personalized dark patterns in Indonesian e-commerce environments. The authors also acknowledge the support of colleagues and academic peers who provided constructive feedback during the development and refinement of this research. Any remaining errors or interpretations are the sole responsibility of the authors.

Author Contributions

Conceptualization: Yudha Erlangga Hidayat; Nurul Citra Fitri Manurung

Data curation: Yudha Erlangga Hidayat

Formal analysis: Yudha Erlangga Hidayat; Nurul Citra Fitri Manurung

Investigation: Yudha Erlangga Hidayat; Nurul Citra Fitri Manurung

Methodology: Yudha Erlangga Hidayat; Nurul Citra Fitri Manurung

Project administration: Yudha Erlangga Hidayat

Supervision: Nurul Citra Fitri Manurung

Validation: Nurul Citra Fitri Manurung

Visualization: Yudha Erlangga Hidayat

Writing - original draft: Yudha Erlangga Hidayat

Writing - review and editing: Yudha Erlangga Hidayat; Nurul Citra Fitri Manurung

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. All research activities were conducted using the authors' own resources.

Conflict of Interest

The authors declare that they have no conflict of interest related to this manuscript.

Statement on the Use of Artificial Intelligence

The authors used ChatGPT to assist with language refinement, grammatical correction, improvement of clarity and academic expression, and organization of selected manuscript sections. AI tools were not used to generate, alter, or fabricate research data, participant responses, analytical findings, or research conclusions. All AI-assisted output was reviewed and verified by the authors, who take full responsibility for the originality, legal reasoning, accuracy, citation verification, confidentiality, research ethics, and final content of the manuscript.

References

- Akbar, M. B., Ibrahim, I., Nabil, S. J., Iqbal, K. A., & Islam, A. K. M. S. (2024). The influence of artificial intelligence on consumer trust in e-commerce: Opportunities and ethical challenges. *European Journal of Theoretical and Applied Sciences*, 2(6). [https://doi.org/10.59324/ejtas.2024.2\(6\).20](https://doi.org/10.59324/ejtas.2024.2(6).20)
- Az-Zahra, P. N., Nurlaily, N., & Agustianto, A. (2025). Regulating dark patterns in Indonesian e-commerce: Comparative lessons from South Korea and the EU. *Journal of Judicial Review*, 27(2), 421-452. <https://doi.org/10.37253/jjr.v27i2.11304>
- Berens, B. M., Bohlender, M., Dietmann, H., Krisam, C., Kulyk, O., & Volkamer, M. (2024). Cookie disclaimers: Dark patterns and lack of transparency. *Computers & Security*, 136, 103507. <https://doi.org/10.1016/j.cose.2023.103507>
- Brenncke, M. (2024). A theory of exploitation for consumer law: Online choice architectures, dark patterns, and autonomy violations. *Journal of Consumer Policy*, 47(1), 127-164. <https://doi.org/10.1007/s10603-023-09554-7>
- De Conca, S. (2023). The present looks nothing like the Jetsons: Deceptive design in virtual assistants and the protection of the rights of users. *Computer Law & Security Review*, 51, 105866. <https://doi.org/10.1016/j.clsr.2023.105866>
- Deligoz, K. (2025). Consumer manipulation with artificial intelligence: Dark patterns and hidden techniques. In *Artificial intelligence and consumer behaviour*. Ozgur Publications. <https://doi.org/10.58830/ozgur.pub710.c3029>
- Farronato, C., Fradkin, A., & Lin, T. (2025). Designing consent: Choice architecture and consumer welfare in data sharing. *Proceedings of the ACM Conference on Economics and Computation*. <https://doi.org/10.1145/3736252.3742627>
- Gorjanc, M. (2025). Trust in the age of artificial intelligence: A framework for privacy protection in personalised marketing. *Journal of Innovative Business and Management*, 17(1). <https://doi.org/10.32015/jibm.2025.17.1.9>

- Gray, C. M., Gunawan, J. T., Schafer, R., Bielova, N., Sanchez Chamorro, L., Seaborn, K., & Mildner, T. (2024). Mobilizing research and regulatory action on dark patterns and deceptive design practices. *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. <https://doi.org/10.1145/3613905.3636310>
- Gray, C. M., Santos, C., Mildner, T., Rossi, A., & Sinderson, C. (2023). Dark patterns and the emerging threats of deceptive design practices. *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. <https://doi.org/10.1145/3544549.3583173>
- Hassan, N., Abdelraouf, M., & El-Shihy, D. (2025). The moderating role of personalized recommendations in the trust-satisfaction-loyalty relationship: An empirical study of AI-driven e-commerce. *Future Business Journal*, 11, 66. <https://doi.org/10.1186/s43093-025-00476-z>
- Hayati, A. N. (2025). The issue of dark patterns in digital platforms: The challenge for Indonesia's consumer protection law. *Asian Journal of Law and Society*. <https://doi.org/10.1017/als.2024.24>
- Herman, J. H. (2024). Dark patterns: EU's regulatory efforts. *Security and Privacy*. <https://doi.org/10.1002/spy2.441>
- Ide, Y., & Beddoe, L. (2023). Challenging perspectives: Reflexivity as a critical approach to qualitative social work research. *Qualitative Social Work*. <https://doi.org/10.1177/14733250231173522>
- Jayapal, J. (2025). Unveiling the impact of AI-driven personalization on customer loyalty in online shopping: The moderating effects of privacy concerns. *Journal of Promotion Management*, 31(5), 865-894. <https://doi.org/10.1080/10496491.2025.2525099>
- Kahlke, R., O'Brien, B. C., & Varpio, L. (2025). Qualitative research interviews for health professions education: AMEE Guide No. 185. *Medical Teacher*. <https://doi.org/10.1080/0142159X.2025.2536697>
- Kelly, D., & Rubin, V. L. (2024). Identifying dark patterns in user account disabling interfaces: Content analysis results. *Social Media + Society*, 10(1). <https://doi.org/10.1177/20563051231224269>
- Kim, W. G., & Lee, M. (2023). Impact of dark patterns on consumers' perceived fairness and attitude: Moderating effects of types of dark patterns, social proof, and moral identity. *Tourism Management*, 98, 104763. <https://doi.org/10.1016/j.tourman.2023.104763>
- Kocyigit, E., Rossi, A., & Lenzini, G. (2023). Towards assessing features of dark patterns in cookie consent processes. In *Privacy Technologies and Policy*. Springer. https://doi.org/10.1007/978-3-031-31971-6_13
- Koh, W. C., & Seah, Y. Z. (2023). Unintended consumption: The effects of four e-commerce dark patterns. *Cleaner and Responsible Consumption*, 11, 100145. <https://doi.org/10.1016/j.clrc.2023.100145>
- Meirezaldi, O. (2025). Dark patterns reconsidered: A cross-taxonomic and conceptual mapping for ethical interface design. *Telaah Bisnis*, 26(1). <https://doi.org/10.35917/tb.v26i1.586>
- Mills, S. (2024). Deceptive choice architecture and behavioral audits: A principles-based approach. *Regulation & Governance*, 18(4), 1426-1441. <https://doi.org/10.1111/rego.12590>
- Piduru, B. R. (2023). Dark patterns in customer experience: Techniques, consequences, and ethical dimensions. *International Journal of Research in Computer Applications and Information Technology*, 5(1), 28-57. <https://doi.org/10.17605/OSF.IO/N3T4D>
- Richardson, P. S., & Fang, B. (2025). Dark patterns or predictive design: An assessment of the Amazon Buy Box. *The BRC Academy Journal of Business*, 14(1). <https://doi.org/10.15239/j.brcacadjb.2025.14.01.ja08>
- Rossi, A., Carli, R., Botes, M. W., Fernandez, A., Sergeeva, A., & Sanchez Chamorro, L. (2024). Who is vulnerable to deceptive design patterns? A transdisciplinary perspective on the

- multi-dimensional nature of digital vulnerability. *Computer Law & Security Review*, 55, 106031. <https://doi.org/10.1016/j.clsr.2024.106031>
- Santos, C., Morozovaite, V., & De Conca, S. (2025). No harm no foul: How harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. *Information & Communications Technology Law*. <https://doi.org/10.1080/13600834.2025.2461958>
- Sarkar, M. (2024). Explainable AI in e-commerce: Enhancing trust and transparency in AI-driven decisions. *Information Technology and Engineering Journal*, 2(1). <https://doi.org/10.70937/itej.v2i01.53>
- Seaborn, K., Itagaki, T., Wang, Y., Geng, P., Fujii, T., Mandai, Y., Kojima, M., & Yoshida, S. (2024). Deceptive, disruptive, no big deal: Japanese people react to simulated dark commercial patterns. *Proceedings of the CHI Conference on Human Factors in Computing Systems*. <https://doi.org/10.1145/3613905.3651099>
- Singh, N. (2023). AI-driven personalization in eCommerce advertising. *International Journal for Research in Applied Science and Engineering Technology*. <https://doi.org/10.22214/ijraset.2023.57695>
- Singh, V., Vishvakarma, N. K., & Kumar, V. (2024). Unveiling digital manipulation and persuasion in e-commerce: A systematic literature review of dark patterns and digital nudging. *Journal of Internet Commerce*, 23(2), 144-171. <https://doi.org/10.1080/15332861.2024.2330813>
- Spais, G., Phau, I., & Jain, V. (2024). AI marketing and AI-based promotions impact on consumer behavior and the avoidance of consumer autonomy threat. *Journal of Consumer Behaviour*, 23(3), 1053-1056. <https://doi.org/10.1002/cb.2248>
- Strunel, A.-M., & Cordoba, S. (2025). Insider/outsider dynamics: A reflexive thematic analysis of reflexivity/positionality in the *Qualitative Research in Psychology* journal. *Qualitative Research in Psychology*. <https://doi.org/10.1080/14780887.2025.2505460>
- Sylviana, G., Maharani, D. P., & Wibowo, A. M. (2025). Keabsahan praktik dark patterns terhadap pemerolehan persetujuan pemrosesan data pribadi di Indonesia. *Rechtjiva*, 2(1). <https://doi.org/10.21776/rechtjiva.v2n1.5>
- Syam, S. (2025). A systematic literature review on the role of artificial intelligence in digital marketing strategies. *International Journal of Economics and Digitalization*, 5(1). <https://doi.org/10.54065/ijed.5.1.2025.335>
- Terry, G., & Hayfield, N. (2025). Reflexive thematic analysis and men's embodiment following injury or illness: A worked example. *Anatomical Sciences Education*. <https://doi.org/10.1002/ase.70058>
- Thukral, A., Aggarwal, N., Garg, A., & Lipika. (2025). A systematic review on dark patterns: Whisper in clicks, hide in links. *International Journal of Global Research Innovations & Technology*, 3(3). <https://doi.org/10.62823/ijgrit/03.03.7864>
- Torres-Quintero, A., & Granados-Garcia, A. (2023). Claves para una practica reflexiva en la investigacion social cualitativa. *Athenea Digital*, 23(1). <https://doi.org/10.5565/rev/athenea.3280>
- Trzaskowski, J. (2024). Manipulation by design. *Electronic Markets*, 34, 14. <https://doi.org/10.1007/s12525-024-00699-y>
- Turki, H. (2025). AI-powered personalization in e-commerce: Governance, consumer behavior, and exploratory insights from big data analytics. *Technology in Society*, 83, 103033. <https://doi.org/10.1016/j.techsoc.2025.103033>
- Uceng, A., & Hanifah, A. M. Z. (2024). Dark patterns and consumer decision making in emerging markets: Experimental evidence from Indonesia. *Data*, 2(3). <https://doi.org/10.61978/data.v2i3.919>
- Udayanga, S. (2025). Reflexive and iterative thematic analysis (RITA): A design-framework for qualitative research. *Qualitative Research*. <https://doi.org/10.1177/14687941251377282>

- Zac, A., Huang, Y.-C., von Moltke, A., Decker, C., & Ezrachi, A. (2025). Dark patterns and consumer vulnerability. *Behavioural Public Policy*. <https://doi.org/10.1017/bpp.2024.49>
- Zahratunnissa, H. S., Etiveni, I., Purwandari, B., & Purwaningsih, E. H. (2025). How people recognize dark pattern in e-commerce? *Jurnal Sistem Informasi*, 21(1), 82-97. <https://doi.org/10.21609/jsi.v21i1.1479>