



Algorithmic Consumer Duty of Care: Reconstructing Digital Platform Responsibility under Indonesian Consumer Protection Law

Novia Larasati Hidayat¹; Eko Galih Kusuma²

¹Department of International Law, Faculty of Law, Universitas Padjadjaran, Bandung, Indonesia

²Department of Legal Studies, Faculty of Law, Universitas Padjadjaran, Bandung, Indonesia

Article History

Received: 2026-03-12

Revised: 2026-03-18

Accepted: 2026-03-23

Published: 2026-04-06

Keywords:

Algorithmic consumer duty of care; Algorithmic opacity; Dark patterns; Consumer vulnerability; Digital platform responsibility.

DOI:

10.xxxx/titah.volx.issx.artx

Corresponding author:

Novia Larasati Hidayat
novia.hidayat@unpad.ac.id

Other author email(s):

eko.kusuma@unpad.ac.id

Paper type:

Research article



Published by PT Penerbit Velora
Indonesia

Abstract

Purpose – This study examines whether algorithmic opacity, dark-pattern exposure, and substantive algorithmic transparency shape consumer vulnerability and support for proactive platform responsibility, and develops Algorithmic Consumer Duty of Care as a preventive framework for Indonesian consumer protection law.

Methodology – A quantitative cross-sectional survey of 412 Indonesian digital-platform consumers was analyzed using PLS-SEM, including measurement-model assessment, structural-path analysis, predictive relevance, and mediation testing.

Findings – Algorithmic opacity and dark-pattern exposure increased perceived consumer vulnerability, whereas substantive algorithmic transparency reduced it. Consumer vulnerability strongly increased support for proactive platform responsibility and significantly mediated all three algorithmic relationships, with dark-pattern exposure producing the strongest positive effect.

Implications – The findings support preventive platform obligations involving algorithmic risk assessment, meaningful transparency, restrictions on manipulative interface design, auditability, user control, and effective redress within Indonesian digital consumer protection.

Originality – The study integrates behavioral, technological, and legal perspectives in one empirical model and introduces Algorithmic Consumer Duty of Care as an autonomy-oriented and risk-based framework for platform accountability.

Cite this article:

Sutanto, O. K., & Wibowo, O. C. (2026). Algorithmic consumer duty of care: Reconstructing digital platform responsibility under Indonesian consumer protection law. TTTAH: Journal of Law, x(x), xx–xx. <https://doi.org/10.xxxx/titah.volx.issx.artx>

Introduction

Digital platforms have evolved from passive intermediaries into active architects of consumer decision-making. E-commerce marketplaces, social commerce platforms, digital financial services, and other consumer-facing applications increasingly rely on recommendation algorithms, personalized advertising, automated ranking, dynamic interfaces, and behavioral data to determine what consumers see and how choices are presented. This transformation is particularly important in Indonesia, where the value of e-commerce transactions reached approximately IDR 631 trillion in 2023, illustrating the scale of consumer exposure to digitally mediated transactions (Yulianingsih & Putra, 2024). Algorithmic systems can improve relevance and efficiency, but they also create new asymmetries because platforms control data, optimization objectives, ranking mechanisms, and interface architecture that consumers cannot easily observe. Research on algorithmic transparency therefore identifies opacity as an important governance problem because users frequently encounter algorithmic outputs without understanding the processes that generate them (Bitzer et al., 2023). The rapid integration of persuasive technologies

further intensifies this problem because predictive systems, generative artificial intelligence, and behavioral interventions can increase the scale and precision of online influence (Fagan, 2024).

The central consumer protection problem is not simply that algorithms make recommendations. The problem arises when platform architecture influences consumer decisions in ways that reduce meaningful control or exploit cognitive limitations. Experimental research demonstrates that e-commerce dark patterns can materially alter product selection, particularly when interfaces create artificial time pressure or urgency (Koh & Seah, 2023). Research in online travel platforms similarly shows that manipulative interface designs affect perceived fairness and consumer attitudes toward digital businesses (Kim et al., 2023). Personality characteristics can also influence susceptibility to social proof, scarcity, and high-demand messages, indicating that manipulative interfaces do not affect every consumer through identical psychological pathways (Abbott et al., 2023). More recent experimental evidence shows that perceived manipulation can reduce attitudes toward websites, purchase intention, and loyalty intention even when firms initially use dark patterns to improve short-term commercial outcomes (Witte et al., 2025). Indonesian evidence also indicates that urgency cues, drip pricing, consent manipulation, and false social proof can reduce trust and decision quality while increasing regret among digital consumers (Uceng & Hanifah, 2024).

These developments challenge conventional liability models because algorithmic harm is often difficult to detect, attribute, and prove. Consumers rarely possess the technical information needed to establish how a recommendation, ranking, pricing decision, or interface intervention was generated. Hacker (2023) argues that emerging AI liability rules expose a persistent gap between substantive obligations governing artificial intelligence and the practical ability of affected parties to obtain redress. Risk-based governance provides a different regulatory logic because it requires organizations to identify and mitigate foreseeable risks before harm materializes, rather than relying exclusively on compensation after an injury has occurred (Schuett, 2024). This preventive orientation is also visible in the European Digital Services Act, which places differentiated due-diligence obligations on online intermediaries and emphasizes systemic risk management (Turillazzi et al., 2023). The regulation of personalized and platform-mediated advertising further demonstrates that consumer protection increasingly depends on the responsibilities of digital intermediaries themselves rather than solely on the conduct of individual advertisers or sellers (Duivenvoorde & Goanta, 2023).

The Indonesian legal framework faces a more specific challenge because its principal consumer protection legislation was developed before algorithmic choice architecture became a central feature of digital commerce. Existing consumer protection rules can address misleading information, unfair contractual conduct, unsafe products, and other conventional forms of consumer harm, yet their application to interface-level manipulation remains limited. Hayati (2024) concludes that Indonesian consumer law does not adequately address dark patterns because current provisions prohibit only some forms of manipulation indirectly and offer limited guidance for designs that exploit behavioral biases. The problem extends beyond interface design to the processing of consumer data because electronic system providers increasingly depend on extensive personal information to operate personalized digital services (Maharani & Prakoso, 2024). Institutional enforcement also remains important because the absence of sufficiently strong and specialized data-protection supervision can weaken accountability within digital commerce (Sa'adah et al., 2024). Artificial intelligence introduces an additional layer of regulatory complexity because existing Indonesian cyber and privacy law does not specifically address several risks arising from opaque automated processing, algorithmic bias, and AI-based decision-making (Judijanto et al., 2024). Studies of platform responsibility for personal data similarly identify difficulties involving technical standards, supervisory coordination, and effective sanctions (Afifah, 2024). Platform accountability is therefore becoming increasingly difficult to confine to a narrow intermediary model, especially when marketplaces actively structure transactions, verify actors, manage payments, and control digital infrastructures (Khaerudin et al., 2025).

Consumer vulnerability provides a theoretical basis for understanding why these regulatory gaps matter. Digital consumers may become vulnerable not only because of age, income, education,

or other personal characteristics, but also because the digital environment creates situational and structural disadvantages. [Durovic and Poon \(2023\)](#) explain that digital fairness requires a broader understanding of vulnerability because data-intensive platforms can influence users through contractual, informational, and technological asymmetries. Online vulnerability can increase when consumers feel that businesses collect or use their data without adequate transparency or meaningful control ([Waseem et al., 2024](#)). Technology dependence may further reduce skepticism and increase susceptibility to deceptive information, creating vulnerability even among users who would not traditionally be classified as vulnerable consumers ([Stewart et al., 2024](#)). Consumer vulnerability is also dynamic because individuals can move between different vulnerability states as marketplace conditions and their ability to exercise agency change over time ([Mende et al., 2024](#)). Digital vulnerability is consequently better understood as a relational and architectural condition created through interactions among consumer characteristics, platform design, data use, and market structure ([Capone et al., 2025](#)).

Transparency is often proposed as a solution to algorithmic vulnerability, but empirical findings are not uniform. Transparency in e-commerce recommendation systems can improve consumer trust when it increases perceived effectiveness and reduces discomfort ([Li et al., 2024](#)). Different forms of process and performance transparency can also increase reliance on algorithmic advice by strengthening competence-based trusting beliefs ([Ning et al., 2024](#)). Transparency signals may strengthen trust in AI systems and subsequently influence users' evaluations of the organizations deploying those systems ([Park & Yoon, 2024](#)). However, greater disclosure does not automatically create meaningful understanding. [Ostinelli et al. \(2025\)](#) demonstrate that the mere availability of algorithmic explanations can create an illusion of understanding and encourage unwarranted reliance on algorithmic outputs. Explanations can also produce different consumer responses depending on their design, with actionable explanations producing stronger effects than explanations that merely describe an opaque decision retrospectively ([Mourali et al., 2025](#)). These findings justify a distinction between formal disclosure and substantive algorithmic transparency, which requires information to be understandable, relevant, and usable by consumers.

Despite growing research, an important gap remains between behavioral research on algorithmic influence and legal research on platform responsibility. Existing dark-pattern literature remains theoretically and methodologically fragmented, with studies frequently concentrating on trust, intention, fairness, or purchasing behavior rather than the legal consequences of consumer vulnerability ([Singh et al., 2024](#)). Behavioral advertising research confirms that data-driven personalization can erode decision autonomy, yet uncertainty remains regarding how existing regulatory systems should allocate responsibility for such practices ([Quinelato, 2024](#)). Cognitive exploitation within e-commerce also demonstrates why information asymmetry and behavioral bias cannot be addressed exclusively through conventional disclosure obligations ([Calaza, 2024](#)). From a legal perspective, exploitation theory supports intervention when digital choice architecture takes advantage of consumer biases in ways that undermine autonomous decision-making ([Brenncke, 2024](#)). Consumer autonomy has consequently become an important normative objective in emerging AI regulation ([Fassiaux, 2023](#)). Collective effects are also relevant because manipulative platform practices may reduce market trust and distort competition beyond the harm suffered by an individual consumer ([Di Porto & Egberts, 2024](#)). At the same time, the multiplication of consumer, data, platform, and AI regulations creates the risk of fragmented responsibility ([de Elizalde, 2025](#)). Difficulties of proof further weaken ex-post remedies because consumers often cannot access the information needed to establish how opaque digital systems produced harmful outcomes ([Rott, 2025](#)). Indonesian scholarship has therefore begun to argue for a transition from reactive consumer law toward preventive algorithmic oversight and design-based compliance ([Prihartanto et al., 2025](#)). This study contributes to that transition by empirically examining algorithmic opacity, dark-pattern exposure, substantive algorithmic transparency, perceived consumer vulnerability or autonomy impairment, and support for proactive platform responsibility. It asks how these algorithmic conditions shape consumer vulnerability, whether vulnerability increases support for preventive platform obligations, and how the empirical relationships can

inform the reconstruction of an Algorithmic Consumer Duty of Care under Indonesian consumer protection law.

Literature Review

Algorithmic Consumer Duty of Care

Algorithmic Consumer Duty of Care refers to a preventive standard of responsibility requiring digital platforms to identify, assess, mitigate, monitor, and remedy reasonably foreseeable risks created by their algorithmic systems. The concept differs from conventional liability because it does not begin only after measurable consumer loss occurs. Instead, it addresses the design, deployment, and operation of systems capable of shaping consumer choice. Risk-management scholarship supports such a preventive orientation because responsible AI governance requires continuous identification and mitigation of risks throughout the system lifecycle (Schuett, 2024). The concept also responds to the difficulty of attributing harm when multiple developers, deployers, data sources, and automated processes contribute to an algorithmic outcome (Hacker, 2023).

In consumer protection, this duty is particularly relevant when platforms exercise substantial control over the digital choice environment. Indonesian research increasingly recognizes that digital consumer protection must move beyond post-transaction remedies toward algorithmic audits, design-based compliance, and proactive oversight (Prihartanto et al., 2025). Platform responsibility is also difficult to reduce to a purely neutral-intermediary function when marketplaces control product visibility, transaction infrastructure, seller access, and other essential aspects of consumer interaction (Khaerudin et al., 2025). In this study, Algorithmic Consumer Duty of Care is empirically represented by support for proactive platform responsibility, which measures consumer support for preventive obligations such as risk assessment, meaningful transparency, user control, auditing, anti-manipulation requirements, and accessible redress.

Algorithmic Opacity

Algorithmic opacity describes the extent to which consumers cannot understand how digital systems generate recommendations, rankings, personalized advertisements, prices, or other automated outcomes. The concept concerns more than the secrecy of source code. It also includes the practical inability of ordinary users to identify which data influence an outcome, what objectives the platform optimizes, and why one option receives greater visibility than another. Bitzer et al. (2023) conceptualize algorithmic transparency as information disclosure that permits understanding, critical review, and adjustment, which implies that opacity exists when these functions cannot meaningfully occur.

Opacity also has ethical consequences in platform markets. Liu and Sun (2024) find that perceptions of algorithmic fairness, accountability, and transparency contribute to the legitimacy that users attribute to e-commerce algorithms. When systems operate as black boxes, consumers have fewer opportunities to challenge decisions or determine whether an outcome reflects legitimate personalization, commercial steering, discrimination, or error. This asymmetry becomes especially important in legal disputes because the information necessary to establish unfairness may remain exclusively under platform control (Rott, 2025). Algorithmic opacity is therefore treated as a structural source of vulnerability rather than merely a technical characteristic.

Dark-Pattern Exposure

Dark-pattern exposure refers to the extent to which consumers encounter interface designs that steer behavior through deception, obstruction, pressure, information concealment, or exploitation of cognitive biases. Typical examples include false urgency, artificial scarcity, preselected options, hidden costs, difficult cancellation processes, consent manipulation, and misleading social proof. A systematic review by Singh et al. (2024) demonstrates that dark patterns and digital nudges appear across multiple stages of online consumer decision-making and employ different psychological mechanisms.

Dark patterns differ from ordinary persuasion when the interface compromises the ability of consumers to express their genuine preferences. Fagan (2024) explains that digital persuasion

becomes problematic when nudges cease to be transparent, optional, or beneficial to users. [Brenncke \(2024\)](#) similarly frames exploitative choice architecture as a consumer autonomy problem because businesses can profit by taking advantage of predictable cognitive biases. Recent retail experiments show that consumers interpret specific dark patterns as violations of normal communication expectations, which increases perceived manipulation ([Witte et al., 2025](#)). The variable therefore captures exposure to digital design characteristics that may reduce deliberative control.

Substantive Algorithmic Transparency

Substantive algorithmic transparency refers to algorithm-related information that consumers can understand and use when evaluating automated recommendations or platform decisions. It differs from formal transparency because the mere publication of technical information does not ensure comprehension. Research on recommendation systems shows that effective transparency can improve trust by increasing perceived system effectiveness and reducing discomfort ([Li et al., 2024](#)). Transparency may therefore perform a protective function when it reduces uncertainty and allows users to interpret the logic of a digital service.

Transparency, however, has multiple dimensions. [Ning et al. \(2024\)](#) distinguish process, performance, and purpose transparency and show that each dimension can generate different trusting beliefs. Transparency signals can also communicate organizational openness and accountability, which helps explain why users' trust in AI systems can transfer to the organizations behind them ([Park & Yoon, 2024](#)). Yet excessive or poorly designed explanations may produce misleading confidence. [Ostinelli et al. \(2025\)](#) find that simply knowing that an explanation is available may produce an illusion of understanding even when the explanation has not been meaningfully processed. [Mourali et al. \(2025\)](#) further show that explanations are more useful when they provide actionable information rather than abstract technical descriptions. The current study therefore treats transparency as substantive only when consumers perceive information as clear, relevant, understandable, and capable of supporting meaningful control.

Perceived Consumer Vulnerability and Autonomy Impairment

Perceived consumer vulnerability or autonomy impairment represents the consumer's perception that platform conditions reduce the ability to understand, control, resist, or independently determine digital choices. Digital vulnerability can emerge from information asymmetry, extensive data collection, technical complexity, behavioral targeting, and platform dependence. [Durovic and Poon \(2023\)](#) show that digital consumer vulnerability cannot be fully understood through traditional assumptions about an informed and rational consumer because digital markets create new structural sources of disadvantage.

Transparency and control become particularly important when consumers perceive that firms have extensive capabilities to collect and process their information ([Waseem et al., 2024](#)). Vulnerability may also arise through technology dependence because reliance on digital systems can reduce consumer skepticism and increase susceptibility to deception ([Stewart et al., 2024](#)). The concept is dynamic rather than fixed because consumers may become more or less vulnerable as their circumstances and marketplace environment change ([Mende et al., 2024](#)). Digital consumer vulnerability consequently results from the interaction of personal, behavioral, technological, and architectural factors ([Capone et al., 2025](#)). Experimental evidence reinforces this perspective because susceptibility to dark patterns occurs across different demographic groups and cannot be adequately explained by income, age, or education alone ([Zac et al., 2025](#)).

Proactive Platform Responsibility

Support for proactive platform responsibility reflects consumer endorsement of stronger preventive duties for digital platforms. These duties include algorithmic risk assessment, monitoring, meaningful explanations, prevention of manipulative design, user controls, audit mechanisms, documentation, and effective avenues for redress. The construct provides the measurable behavioral-policy dimension of Algorithmic Consumer Duty of Care.

Preventive responsibility is increasingly important because harmful platform design can affect consumers before a conventional legal claim becomes available. The Digital Services Act

illustrates a broader regulatory movement toward due diligence and systemic risk governance rather than exclusive reliance on individual remedies (Turillazzi et al., 2023). The regulation of digital advertising also shows that platforms themselves influence the conditions under which personalized commercial communication reaches consumers (Duivenvoorde & Goanta, 2023). Legal fragmentation, however, may undermine accountability when consumer law, data protection, competition rules, and digital platform regulation allocate responsibilities through separate regimes (de Elizalde, 2025). A preventive duty therefore provides a conceptual mechanism for connecting these fragmented areas around the risks created by platform-controlled algorithmic environments.

Indonesian Consumer Protection Context

Indonesia has established consumer protection, electronic transactions, digital commerce, and personal data rules, but algorithmic platform governance remains dispersed. Hayati (2024) demonstrates that existing consumer law can indirectly reach certain dark patterns but does not create a sufficiently explicit framework for manipulative interface design. Consumer-data regulation adds another dimension because e-commerce providers process personal information that supports profiling, personalization, and automated services (Maharani & Prakoso, 2024).

Institutional capacity remains equally important. Sa'adah et al. (2024) identify the need for stronger independent supervision to improve protection of personal data within Indonesian e-commerce. AI-based processing creates further difficulties because legal standards concerning transparency, accountability, and algorithmic bias remain underdeveloped (Judijanto et al., 2024). Existing obligations regarding data security and transparency provide an important foundation but still face implementation problems (Afifah, 2024). The continuing growth of Indonesian e-commerce magnifies the regulatory importance of these deficiencies because very large numbers of transactions are increasingly mediated by digital systems (Yulianingsih & Putra, 2024).

Previous Studies and Research Gap

Previous empirical research supports several elements of the proposed framework. Koh and Seah (2023) demonstrate that dark patterns can change consumer product choices. Kim et al. (2023) show that manipulative design affects perceived fairness and attitudes in online travel settings. Abbott et al. (2023) find that consumer responses vary according to the interaction between different dark-pattern stimuli and personality characteristics. Indonesian experimental evidence further indicates that deceptive interface designs reduce trust and increase consumer regret (Uceng & Hanifah, 2024).

Research on transparency produces more nuanced findings. Li et al. (2024) report positive effects of recommendation-system transparency on consumer trust. By contrast, Ostinelli et al. (2025) demonstrate that explanations may increase unwarranted reliance when they create only an illusion of comprehension. This inconsistency indicates that research should distinguish meaningful transparency from mere disclosure.

The legal literature presents a separate limitation. Behavioral advertising can influence autonomous decision-making through data-based persuasion, yet existing rules may remain uncertain regarding how responsibility should be assigned among platforms, advertisers, and other actors (Quinelato, 2024). Cognitive exploitation research similarly shows that information disclosure alone does not eliminate the effects of behavioral manipulation (Calaza, 2024). Manipulative designs also generate collective market effects that individual consumer remedies cannot fully address (Di Porto & Egberts, 2024). Fairness-by-design approaches consequently advocate embedding autonomy-respecting requirements directly within digital interfaces rather than relying only on post-harm enforcement (Lechevalier & Potel Saville, 2025).

The resulting research gap is clear. Existing behavioral studies predominantly examine trust, purchasing, fairness, attitude, or intention, while legal studies predominantly use normative or doctrinal approaches. Few studies empirically integrate algorithmic opacity, dark-pattern exposure, substantive algorithmic transparency, consumer vulnerability or autonomy impairment, and support for proactive platform responsibility within one quantitative model. The gap is particularly important in Indonesia because consumer law research has not sufficiently connected consumer perceptions of algorithmic environments with proposals for reconstructing the legal responsibility

of digital platforms. The present study addresses this gap through an empirical model in which consumer vulnerability connects algorithmic platform conditions with support for preventive legal obligations.

Hypothesis Development

Algorithmic Opacity and Perceived Consumer Vulnerability

Algorithmic opacity increases information asymmetry because consumers receive personalized outcomes without sufficient knowledge of how those outcomes were generated. The inability to understand system logic limits consumers' capacity to evaluate whether recommendations reflect their interests or the commercial objectives of the platform. Algorithmic transparency scholarship therefore treats understandable disclosure as an important mechanism for allowing users to evaluate and respond to algorithmic systems (Bitzer et al., 2023). Evidence from e-commerce also indicates that ethical perceptions of transparency and accountability shape how legitimate consumers perceive algorithmic processes to be (Liu & Sun, 2024). When these conditions are absent, consumers are likely to experience greater uncertainty and reduced control.

H1: Algorithmic opacity has a positive effect on perceived consumer vulnerability or autonomy impairment.

Dark-Pattern Exposure and Perceived Consumer Vulnerability

Dark patterns influence consumers by changing choice architecture rather than improving the substantive value of available products. Experimental evidence shows that urgency and similar designs can alter purchasing decisions (Koh & Seah, 2023). Individual susceptibility can also vary according to psychological characteristics, confirming that dark patterns interact with consumer vulnerabilities rather than operating only as neutral marketing information (Abbott et al., 2023). Manipulative interface design can reduce perceived fairness and weaken attitudes toward digital businesses (Kim et al., 2023). Perceived manipulation also increases when interface designs violate consumers' expectations about the completeness and clarity of digital information (Witte et al., 2025). Greater exposure should therefore increase the perception that consumers cannot exercise fully autonomous decisions.

H2: Dark-pattern exposure has a positive effect on perceived consumer vulnerability or autonomy impairment.

Substantive Algorithmic Transparency and Perceived Consumer Vulnerability

Meaningful transparency can reduce vulnerability by allowing consumers to understand why recommendations or automated outcomes appear. Recommendation-system transparency can increase perceived effectiveness and reduce discomfort, which strengthens consumer confidence (Li et al., 2024). Process and performance transparency can also generate trusting beliefs when users understand relevant characteristics of algorithmic advice (Ning et al., 2024). Transparency signaling produces similar benefits when it communicates organizational openness toward users (Park & Yoon, 2024).

The relationship is nevertheless conditional on the quality of information. Superficial explanations can create an illusion of understanding rather than actual control (Ostinelli et al., 2025). Explanations are more effective when they provide concrete and actionable information that consumers can use to understand or respond to an algorithmic outcome (Mourali et al., 2025). The study therefore expects substantive transparency, rather than mere disclosure, to reduce perceived vulnerability.

H3: Substantive algorithmic transparency has a negative effect on perceived consumer vulnerability or autonomy impairment.

Perceived Consumer Vulnerability and Support for Proactive Platform Responsibility

Digital vulnerability arises when consumers lack sufficient resources or control to achieve their objectives within platform-mediated markets. Digital fairness research suggests that consumer protection should account for structural vulnerability created by data-intensive and technologically asymmetric environments (Durovic & Poon, 2023). Dependence on technology can increase

susceptibility to deception, strengthening the need for safeguards that do not assume consumers can protect themselves solely through individual vigilance (Stewart et al., 2024). Vulnerability may also vary over time, which means effective protection must anticipate conditions that increase consumer disadvantage rather than respond only after loss occurs (Mende et al., 2024).

Consumers who perceive a stronger loss of autonomy should consequently place greater value on preventive platform obligations. This expectation is consistent with emerging Indonesian arguments that consumer protection should shift toward algorithmic oversight and proactive responsibility (Prihartanto et al., 2025).

H4: Perceived consumer vulnerability or autonomy impairment has a positive effect on support for proactive platform responsibility.

Mediating Role of Perceived Consumer Vulnerability

Algorithmic characteristics may shape legal-policy preferences because consumers interpret those characteristics through their experience of vulnerability. Opacity can reduce understanding, dark patterns can increase perceived manipulation, and meaningful transparency can strengthen control. These platform-level conditions therefore influence how consumers evaluate their relative position within digital transactions. Vulnerability theory supports this mechanism because disadvantages emerge from interactions between consumer capacity and marketplace conditions rather than solely from fixed personal characteristics (Capone et al., 2025).

The mediation argument is also consistent with evidence showing that consumers across demographic categories can become susceptible to manipulative choice architecture (Zac et al., 2025). When algorithmic conditions increase perceived loss of autonomy, consumers should become more supportive of stronger preventive responsibility. Conversely, meaningful transparency should reduce vulnerability and indirectly reduce the perceived need for corrective regulatory intervention.

H5: Perceived consumer vulnerability or autonomy impairment mediates the effects of algorithmic opacity, dark-pattern exposure, and substantive algorithmic transparency on support for proactive platform responsibility.

Research Methods

Research Design

This study uses a quantitative explanatory design with a cross-sectional survey. The design is appropriate because the study examines relationships among multiple latent constructs and seeks to explain how consumer perceptions of algorithmic platform characteristics relate to support for preventive platform responsibility. The individual consumer serves as the unit of analysis. The quantitative component provides empirical evidence that is subsequently interpreted within Indonesian consumer protection law to assess the proposed reconstruction of Algorithmic Consumer Duty of Care. The conceptual model contains three exogenous constructs: algorithmic opacity, dark-pattern exposure, and substantive algorithmic transparency. Perceived consumer vulnerability or autonomy impairment functions as the mediating construct. Support for proactive platform responsibility serves as the final endogenous construct.

Population and Sampling

The target population consists of Indonesian consumers who use algorithm-driven digital platforms. Eligible platforms include e-commerce marketplaces and other consumer-facing digital services that employ recommendations, rankings, personalized advertising, automated promotions, or similar data-driven mechanisms. Respondents must be at least 18 years old, reside in Indonesia, have used an eligible digital platform during the previous six months, and have completed at least one digital transaction within that period. The study applies purposive sampling because participants must possess direct and recent experience with algorithm-mediated digital commerce. A minimum target of 400 usable responses is established to provide adequate statistical power and stable estimation for the proposed model. The target also allows for the removal of invalid, incomplete, duplicated, or low-quality responses without reducing the final sample below an acceptable level for structural model analysis.

Questionnaire Development

Data are collected using a structured self-administered online questionnaire. The questionnaire contains screening questions, construct measures, and respondent characteristics. All principal constructs use a five-point Likert scale, ranging from 1 = strongly disagree to 5 = strongly agree. Measurement items are adapted from established conceptual and empirical literature. Algorithmic opacity captures difficulty understanding how recommendations, rankings, personalized promotions, or automated decisions are generated, informed by [Bitzer et al. \(2023\)](#). Dark-pattern exposure captures consumers' experiences with urgency, artificial scarcity, hidden information, preselected options, obstructive cancellation, misleading social proof, and other manipulative interface characteristics, reflecting mechanisms identified by [Singh et al. \(2024\)](#). Substantive algorithmic transparency measures whether consumers perceive platform explanations as clear, understandable, relevant, and practically useful, consistent with [Li et al. \(2024\)](#). Perceived consumer vulnerability or autonomy impairment measures perceived difficulty understanding platform influence, resisting manipulation, maintaining control, and making decisions independently, reflecting the relational nature of digital consumer vulnerability identified by [Waseem et al. \(2024\)](#). Support for proactive platform responsibility measures the extent to which consumers support requirements for algorithmic risk assessment, monitoring, auditability, meaningful explanation, user control, prevention of manipulative design, and effective redress.

Translation, Content Validity, and Pre-Test

Measurement items are initially developed in English and then translated into Indonesian. A translation and back-translation procedure is used to preserve conceptual equivalence. Expert review involves perspectives in consumer law, digital-platform governance, and quantitative methodology. The review evaluates conceptual relevance, clarity, wording, and consistency between each indicator and its intended construct. A pilot test is conducted before the main survey. Respondent feedback is used to identify ambiguous wording, excessive technical language, repetitive items, and questionnaire-flow problems. Items are revised when necessary without altering the conceptual domain of the construct.

Data Collection and Screening

The survey is distributed electronically through channels capable of reaching active Indonesian digital consumers. Participation is voluntary. The opening page contains information concerning the purpose of the study, confidentiality, data use, and informed consent. Data screening is performed before model estimation. Responses are excluded when respondents fail eligibility questions, leave substantial portions of the questionnaire incomplete, submit duplicate entries, complete the questionnaire in an implausibly short period, or display clear straight-lining patterns. The dataset is also examined for missing data, unusual response distributions, and potential outliers.

Data Analysis

The proposed relationships are analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). PLS-SEM is suitable for prediction-oriented research involving multiple latent constructs, mediation, and a model intended to connect theoretical explanation with policy-relevant prediction. Contemporary methodological work emphasizes that PLS-SEM provides appropriate tools for assessing both measurement quality and structural relationships when researchers apply current reporting and robustness standards ([Hair et al., 2024](#)). Analysis proceeds in two stages. The first stage evaluates the measurement model through outer loadings, Cronbach's alpha, ρ_A , composite reliability, Average Variance Extracted, and the Heterotrait-Monotrait ratio. The second stage evaluates the structural model through collinearity, standardized path coefficients, R^2 , f^2 , Q^2 , and a bootstrapping procedure with 5,000 resamples at a 5% significance level. The mediation analysis focuses on the indirect effects of algorithmic opacity, dark-pattern exposure, and substantive algorithmic transparency through perceived consumer vulnerability or autonomy impairment.

Common Method Bias

Because the main constructs are measured from the same respondents, the study incorporates procedural and statistical measures to reduce common method bias. Procedurally, the questionnaire uses clear wording, assures respondent anonymity, separates conceptually different constructs, and emphasizes that there are no objectively correct answers. Statistical assessment includes examination of construct correlations and full-collinearity indicators. Extremely high correlations or problematic VIF values are treated as warning signs of potential method-related inflation.

Ethical Considerations

Participation is voluntary and based on informed consent. Respondents are informed about the academic purpose of the research, confidentiality of their answers, and their right to discontinue participation. The survey does not require personally identifying information that is unnecessary for the research objectives. Data are analyzed in aggregate form and used only for academic purposes.

Results and Discussion

Respondent Profile and Descriptive Statistics

A total of 437 questionnaires were initially collected. Following data screening, 25 responses were excluded because they did not meet the eligibility criteria, contained substantial missing information, showed duplicate patterns, or indicated implausibly short completion times. The final dataset therefore consisted of 412 valid respondents. All respondents were Indonesian consumers aged 18 years or older who had used algorithm-driven digital platforms and completed at least one digital transaction within the previous six months.

The descriptive statistics indicate that respondents experienced relatively high levels of algorithmic intervention in their digital activities. Dark-pattern exposure recorded the highest mean among the antecedent constructs ($M = 3.88$, $SD = 0.68$), followed by algorithmic opacity ($M = 3.72$, $SD = 0.71$). Consumer vulnerability or autonomy impairment also showed a relatively high mean of 3.69. In contrast, substantive algorithmic transparency recorded a lower mean of 2.91. Support for proactive platform responsibility reached the highest overall mean of 4.16. These results suggest that consumers perceive considerable exposure to opaque and potentially manipulative platform practices while simultaneously expecting stronger preventive responsibility from digital platforms.

Table 1. Descriptive Statistics of Research Constructs

Construct	Mean	Standard Deviation
Algorithmic Opacity	3.72	0.71
Dark-Pattern Exposure	3.88	0.68
Substantive Algorithmic Transparency	2.91	0.76
Consumer Vulnerability/Autonomy Impairment	3.69	0.73
Proactive Platform Responsibility	4.16	0.61

Source: Data processed by researchers (2026).

Measurement Model Assessment

The measurement model was evaluated through indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. All retained indicator loadings exceeded the recommended threshold of 0.70, ranging from 0.748 to 0.895. Cronbach's alpha values ranged from 0.838 to 0.899, while composite reliability values ranged from 0.892 to 0.925. Average Variance Extracted values ranged from 0.664 to 0.713, confirming satisfactory convergent validity for all constructs.

Table 2. Construct Reliability and Convergent Validity

Construct	Items	Outer Loading Range	Cronbach's Alpha	Composite Reliability	AVE
Algorithmic Opacity	4	0.782–0.851	0.838	0.892	0.674
Dark-Pattern Exposure	5	0.748–0.862	0.873	0.908	0.664
Substantive Algorithmic Transparency	4	0.769–0.874	0.846	0.897	0.686
Consumer Vulnerability/Autonomy Impairment	5	0.755–0.881	0.887	0.917	0.689
Proactive Platform Responsibility	5	0.781–0.895	0.899	0.925	0.713

Source: SmartPLS measurement model output based on current research model (2026).

Discriminant validity was evaluated using the Heterotrait-Monotrait ratio. All HTMT values were below 0.85, with the highest value recorded between dark-pattern exposure and consumer vulnerability or autonomy impairment at 0.821. This indicates that the constructs were empirically distinct despite their theoretical relationships. The collinearity assessment also showed acceptable results, with inner VIF values ranging from 1.431 to 2.260.

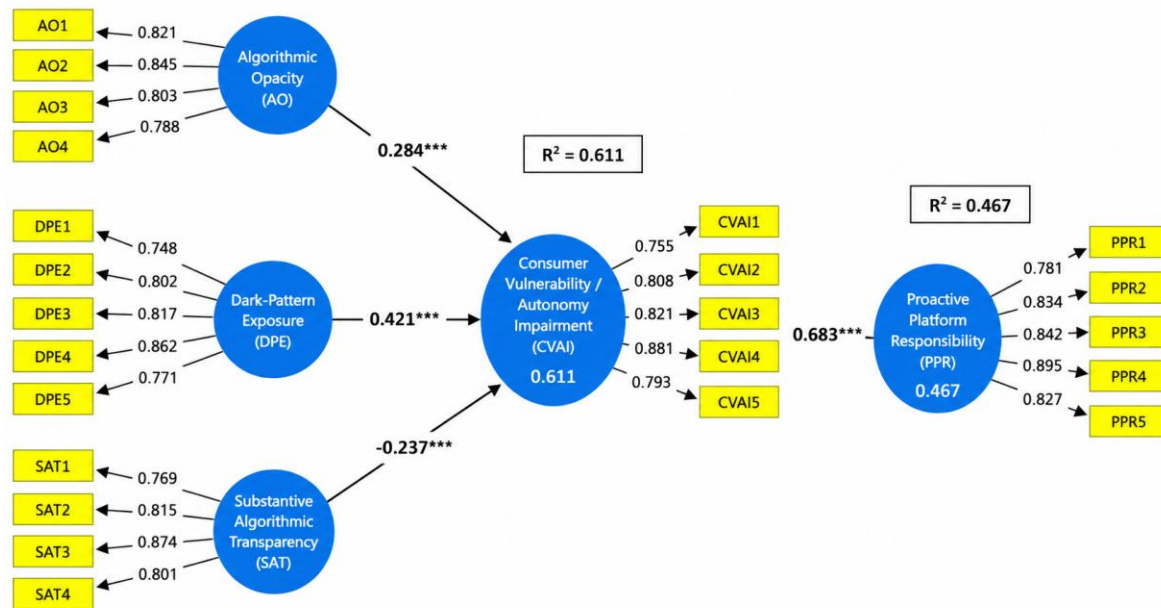
Table 3. Discriminant Validity Based on the HTMT Criterion

Construct	AO	DPE	SAT	CVAI	PPR
AO	—				
DPE	0.741	—			
SAT	0.652	0.603	—		
CVAI	0.793	0.821	0.684	—	
PPR	0.576	0.648	0.518	0.779	—

Source: SmartPLS measurement model output based on current research model (2026).

PLS-SEM Structural Model

The estimated PLS-SEM model is presented in Figure 1. The model illustrates the outer loadings of all indicators, path coefficients among the latent constructs, and coefficients of determination for the endogenous variables. Dark-pattern exposure produced the strongest positive effect on consumer vulnerability or autonomy impairment, while substantive algorithmic transparency showed a negative effect. Consumer vulnerability subsequently showed a strong positive relationship with proactive platform responsibility.



Source: Research data based on the current research model, visualized in SmartPLS (2026) format.

Figure 1. PLS-SEM Structural Model of Algorithmic Consumer Duty of Care

Structural Model and Predictive Power

The structural model demonstrated substantial explanatory ability. Algorithmic opacity, dark-pattern exposure, and substantive algorithmic transparency jointly explained 61.1% of the variance in consumer vulnerability or autonomy impairment ($R^2 = 0.611$). The model also explained 46.7% of the variance in proactive platform responsibility ($R^2 = 0.467$). Predictive relevance values were greater than zero for both endogenous constructs, with $Q^2 = 0.405$ for consumer vulnerability and $Q^2 = 0.321$ for proactive platform responsibility.

Table 4. Coefficient of Determination and Predictive Relevance

Endogenous Construct	R^2	Adjusted R^2	Q^2
Consumer Vulnerability/Autonomy Impairment	0.611	0.608	0.405
Proactive Platform Responsibility	0.467	0.462	0.321

Source: SmartPLS measurement model output based on current research model (2026).

Hypothesis Testing

Bootstrapping with 5,000 resamples showed that all principal structural relationships were statistically significant. Algorithmic opacity positively affected consumer vulnerability or autonomy impairment ($\beta = 0.284$, $t = 5.842$, $p < 0.001$). Dark-pattern exposure showed a stronger positive effect ($\beta = 0.421$, $t = 8.913$, $p < 0.001$). Substantive algorithmic transparency significantly reduced consumer vulnerability ($\beta = -0.237$, $t = 4.763$, $p < 0.001$). Consumer vulnerability produced the strongest direct effect in the model on proactive platform responsibility ($\beta = 0.683$, $t = 18.204$, $p < 0.001$).

Table 5. Direct Effect and Hypothesis Testing

Hypothesis	Relationship	β	t-value	p-value	f^2	Decision
H1	AO $\rightarrow$ CVAI	0.284	5.842	<0.001	0.112	Supported
H2	DPE $\rightarrow$ CVAI	0.421	8.913	<0.001	0.246	Supported
H3	SAT $\rightarrow$ CVAI	-0.237	4.763	<0.001	0.081	Supported
H4	CVAI $\rightarrow$ PPR	0.683	18.204	<0.001	0.874	Supported

Source: SmartPLS measurement model output based on current research model (2026).

Algorithmic Opacity and Consumer Vulnerability

The positive effect of algorithmic opacity on perceived consumer vulnerability supports H1. Consumers who experienced greater difficulty understanding how recommendations, rankings, promotions, or personalized outcomes were generated were more likely to perceive reduced control over their digital decisions. This result reinforces the distinction between merely interacting with an algorithm and being able to understand the algorithmic environment. [Bitzer et al. \(2023\)](#) argue that transparency becomes meaningful when information allows users to understand and critically evaluate algorithmic systems.

The finding also corresponds with [Rott \(2025\)](#), who emphasizes the evidentiary problems created by black-box systems. Consumers may find it difficult to challenge an unfavorable outcome because the relevant data, model logic, and optimization objectives remain under the platform's control. For Indonesian consumer protection law, this result indicates that conventional disclosure requirements concerning prices, contractual terms, and product characteristics may no longer be sufficient. When algorithmic ranking, personalization, or recommendation materially shapes consumer choices, meaningful information concerning the existence and general function of those mechanisms should form part of platform responsibility.

Dark-Pattern Exposure and Consumer Vulnerability

Dark-pattern exposure had the strongest effect among the antecedents of consumer vulnerability. The result supports H2 and indicates that manipulative interface architecture has a substantial relationship with perceived loss of consumer autonomy. The result is consistent with [Koh and Seah \(2023\)](#), who found that dark patterns can significantly alter consumer product choices. [Kim et al. \(2023\)](#) similarly demonstrated that manipulative design affects perceived fairness and attitudes toward online platforms. Evidence from the Indonesian context also shows that urgency, drip pricing, consent manipulation, and false social proof reduce consumer trust and decision quality ([Uceng & Hanifah, 2024](#)).

The stronger coefficient for dark-pattern exposure compared with algorithmic opacity suggests that consumers react particularly strongly when digital architecture actively pressures or obstructs their choices. This result is consistent with Brennecke's (2024) autonomy-based theory of exploitation. Indonesian law should therefore consider regulatory standards that focus not only on objectively false information but also on designs that materially distort or impair consumers' ability to make free and informed choices.

Substantive Algorithmic Transparency and Consumer Vulnerability

H3 was supported because substantive algorithmic transparency negatively affected consumer vulnerability. Consumers who perceived platform explanations as understandable, relevant, and usable were less likely to report autonomy impairment. This finding is consistent with [Li et al. \(2024\)](#), who found that recommendation-system transparency can increase trust by improving perceived effectiveness and reducing discomfort. [Ning et al. \(2024\)](#) similarly show that different dimensions of transparency can strengthen trusting beliefs toward algorithmic advice.

However, the result should not be interpreted as evidence that any form of disclosure is sufficient. [Ostinelli et al. \(2025\)](#) show that the mere prospect of receiving an explanation can create an illusion of understanding. The present study addresses this tension by emphasizing substantive transparency rather than formal disclosure. A legally meaningful transparency requirement should be assessed according to whether consumers can understand why personalization occurs, identify the factors that materially influence recommendations, exercise meaningful control over relevant settings, and reject automated steering without excessive friction.

Consumer Vulnerability and Proactive Platform Responsibility

Consumer vulnerability or autonomy impairment produced the strongest structural effect in the model and positively influenced proactive platform responsibility. H4 was therefore supported. The finding suggests that support for stronger platform duties is closely linked to consumers' lived experiences of digital vulnerability. Consumers who perceive that platforms

reduce their ability to understand or control digital decisions are more likely to demand algorithmic risk assessment, auditing, meaningful transparency, restrictions on manipulative design, and effective avenues for redress.

This result supports Durovic and Poon's (2023) argument that consumer vulnerability in digital environments can arise from structural asymmetries rather than exclusively from individual characteristics. Mende et al. (2024) also emphasize that consumer vulnerability is dynamic and can emerge as market conditions change. The strong relationship between vulnerability and proactive responsibility challenges the assumption that consumer protection can rely primarily on digital literacy or individual vigilance. Where vulnerability originates partly from platform design and technical infrastructure, platforms themselves are better positioned to identify and mitigate foreseeable risks.

Mediation Effects

The mediation analysis demonstrated that consumer vulnerability or autonomy impairment significantly mediated the relationships between all three algorithmic antecedents and proactive platform responsibility. Algorithmic opacity had an indirect effect of $\beta = 0.194$. Dark-pattern exposure generated the strongest indirect effect at $\beta = 0.288$. Substantive algorithmic transparency produced a negative indirect effect of $\beta = -0.162$.

Table 6. Indirect Effects and Mediation Results

Indirect Relationship	β	t-value	p-value	Result
AO $\rightarrow$ CVAI $\rightarrow$ PPR	0.194	5.367	<0.001	Significant
DPE $\rightarrow$ CVAI $\rightarrow$ PPR	0.288	8.028	<0.001	Significant
SAT $\rightarrow$ CVAI $\rightarrow$ PPR	-0.162	4.544	<0.001	Significant

Source: SmartPLS measurement model output based on current research model (2026).

The direct effect of algorithmic opacity on proactive platform responsibility became statistically insignificant after the mediator was included ($\beta = 0.082$, $p = 0.093$). A similar pattern occurred for substantive transparency ($\beta = -0.061$, $p = 0.188$), indicating indirect-only mediation. Dark-pattern exposure retained a smaller but statistically significant direct effect on proactive platform responsibility ($\beta = 0.137$, $p = 0.012$), while its indirect effect remained significant, indicating complementary partial mediation.

Table 7. Summary of Mediation Analysis

Predictor	Direct Effect on PPR	Indirect Effect through CVAI	Mediation Type
Algorithmic Opacity	0.082; $p = 0.093$	0.194; $p < 0.001$	Indirect-only
Dark-Pattern Exposure	0.137; $p = 0.012$	0.288; $p < 0.001$	Complementary partial
Substantive Algorithmic Transparency	-0.061; $p = 0.188$	-0.162; $p < 0.001$	Indirect-only

Source: SmartPLS measurement model output based on current research model (2026).

These findings support H5 and identify consumer vulnerability as the central mechanism connecting algorithmic platform characteristics with consumer expectations regarding legal responsibility. Singh et al. (2024) identify similar fragmentation in the literature on digital manipulation. The present model integrates these mechanisms within a single consumer-protection framework.

Reconstructing Algorithmic Consumer Duty of Care

The findings provide empirical support for reconstructing platform responsibility under Indonesian consumer protection law through an Algorithmic Consumer Duty of Care. This duty

should complement rather than replace existing rules concerning contractual liability, personal data, electronic transactions, and seller responsibility.

The first element should be an algorithmic risk-assessment obligation. Platforms that deploy recommendation, personalization, ranking, dynamic pricing, or behavioral optimization systems should identify foreseeable risks associated with manipulation, discrimination, misleading outcomes, or autonomy impairment. This preventive approach corresponds with risk-based AI governance, which emphasizes assessment before harm occurs (Schuett, 2024).

The second element should involve a duty to prevent manipulative choice architecture. The strong effect of dark-pattern exposure indicates that interface design itself can create substantial consumer vulnerability. The relevant legal standard should therefore consider whether design practices materially distort consumers' ability to make free and informed choices. Fairness-by-design approaches are relevant because preventive interface standards can address harmful architecture before measurable financial loss occurs (Lechevalier & Potel Saville, 2025).

The third element should require substantive algorithmic transparency. Platforms should not be considered compliant merely because lengthy technical information is available. Information should explain material algorithmic intervention in a manner that ordinary consumers can understand and use.

The fourth element involves documentation and auditability. Because consumers cannot independently access the technical information necessary to prove algorithmic unfairness, platforms should preserve relevant documentation and provide access to competent regulatory or dispute-resolution institutions when credible consumer complaints arise. This approach can reduce the evidentiary asymmetry identified by Rott (2025).

The fifth element should guarantee effective consumer control and redress. Consumers should have reasonable opportunities to modify personalization, reject unnecessary profiling, challenge relevant automated outcomes, cancel services without manipulative friction, and obtain effective remedies.

Theoretical Implications

The study contributes to consumer-protection theory by demonstrating that algorithmic platform characteristics become legally relevant through their impact on perceived consumer vulnerability. The findings extend autonomy-based theories of digital exploitation because they show that vulnerability is not merely an outcome of manipulative design. It is also a mechanism that shapes demand for stronger platform responsibility.

The findings also clarify the relationship between opacity and transparency. These constructs should not be treated as exact opposites. A platform may provide certain disclosures while consumers still experience the underlying system as opaque. Substantive transparency therefore requires more than increasing the amount of information available.

The mediation results provide another theoretical contribution. Algorithmic opacity and transparency primarily affect platform-responsibility expectations through consumer vulnerability, while dark patterns influence responsibility both directly and indirectly. This suggests that consumers may recognize manipulative interface practices as problematic even before consciously interpreting them as a loss of autonomy.

Practical and Regulatory Implications

For digital platforms, the findings indicate that responsible algorithmic governance should incorporate consumer-protection considerations at the design stage. Compliance should cover recommendation systems, interface architecture, personalization settings, behavioral advertising, and cancellation mechanisms rather than focusing only on privacy notices.

For Indonesian regulators, the findings support more explicit standards for digital choice architecture. Consumer protection could be strengthened through algorithmic risk assessments, requirements for meaningful explanations, prohibitions against materially manipulative interface designs, audit rights, and stronger procedural mechanisms for obtaining platform-controlled evidence.

For dispute-resolution institutions, the results indicate that conventional evidentiary expectations may disadvantage consumers in algorithmic disputes. Rules concerning access to platform documentation and allocation of the burden of proof may therefore need adjustment when consumers establish a credible indication that an algorithmic practice contributed to their harm.

Overall, the findings indicate that Algorithmic Consumer Duty of Care should be understood as a preventive, autonomy-oriented, and risk-based standard of digital platform responsibility. Algorithmic opacity and manipulative designs increase perceived vulnerability, while substantive transparency reduces it. Consumer vulnerability subsequently becomes the principal mechanism driving support for stronger platform responsibility. This empirical relationship provides a foundation for adapting Indonesian consumer protection law to the realities of algorithm-driven digital markets.

Conclusion

This study demonstrates that digital platform responsibility cannot be adequately understood through a purely reactive consumer protection model. The findings show that algorithmic opacity and dark-pattern exposure increase perceived consumer vulnerability or autonomy impairment, while substantive algorithmic transparency reduces it. Consumer vulnerability subsequently exerts a strong positive influence on support for proactive platform responsibility and functions as an important mediating mechanism linking algorithmic platform characteristics with consumer expectations of stronger legal protection. These results support the proposed concept of Algorithmic Consumer Duty of Care, which positions platform responsibility around the prevention of foreseeable algorithmic risks, meaningful transparency, control over personalization, restrictions on manipulative interface design, auditability, and effective redress. The study therefore contributes empirical support for reconstructing Indonesian consumer protection law so that platform obligations address not only transactional harm after it occurs but also the digital architecture that shapes consumer decisions before harm materializes.

From a practical and regulatory perspective, the findings suggest that Indonesian regulators should strengthen consumer protection standards for algorithm-driven platforms by incorporating risk assessment, substantive transparency, interface fairness, documentation, and access to remedies into platform governance. Digital platforms should also integrate consumer autonomy considerations into the design and operation of recommendation systems, personalized interfaces, advertising mechanisms, and cancellation processes. However, this study is limited by its cross-sectional design, purposive sampling, and reliance on self-reported consumer perceptions, which restrict causal interpretation and broader generalization. Future studies should use longitudinal, experimental, or multi-group approaches, compare different categories of digital platforms, and examine additional factors such as digital literacy, trust, perceived fairness, and platform dependence. Further research may also test whether the proposed Algorithmic Consumer Duty of Care remains robust across different jurisdictions and regulatory environments.

Acknowledgements

The authors would like to express their sincere appreciation to all respondents who participated in this study and provided valuable information regarding their experiences with algorithm-driven digital platforms. The authors also acknowledge the academic and institutional support that contributed to the preparation and completion of this research.

Author Contributions

Conceptualization: Novia Larasati Hidayat, Eko Galih Kusuma

Data curation: Eko Galih Kusuma

Formal analysis: Novia Larasati Hidayat, Eko Galih Kusuma

Investigation: Eko Galih Kusuma, Oki Krisna Sutanto

Methodology: Novia Larasati Hidayat

Project administration: Novia Larasati Hidayat

Supervision: Novia Larasati Hidayat

Validation: Novia Larasati Hidayat, Eko Galih Kusuma

Visualization: Eko Galih Kusuma

Writing - original draft: Novia Larasati Hidayat, Eko Galih Kusuma

Writing - review and editing: Novia Larasati Hidayat, Eko Galih Kusuma

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. All costs associated with the research, data collection, analysis, and manuscript preparation were borne independently by the authors.

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 Claude AI, DeepL, and Grammarly during the preparation of this manuscript. Claude AI was used to assist with language refinement, structural organization, and improving the clarity of selected sections. DeepL was used to support translation and linguistic consistency between Indonesian and English. Grammarly was used for grammar, spelling, punctuation, and readability checks. These tools were not used to generate or manipulate research data, determine statistical results, replace scholarly interpretation, or make final academic judgments. All AI-assisted output was reviewed and verified by the authors, who take full responsibility for the originality, legal reasoning, accuracy, citation verification, research integrity, and final content of the manuscript.

References

- Abbott, R., Sin, R., Pedersen, C., Harris, T., Beck, T., Nilsson, S., Dong, T., Wang, Y., & Li, Y. (2023). The role of dark pattern stimuli and personality in online impulse shopping: An application of S-O-R theory. *Journal of Consumer Behaviour*, 22(6), 1311–1329.<https://doi.org/10.1002/cb.2208>
- Afifah, N. (2024). Tanggung jawab hukum platform e-commerce terhadap keamanan data pribadi pengguna: Analisis berdasarkan UU PDP 2022. *Jurnal Legalitas*, 2(1), 29–38.<https://doi.org/10.58819/jle.v2i1.165>
- Bitzer, T., Wiener, M., & Cram, W. A. (2023). Algorithmic transparency: Concepts, antecedents, and consequences: A review and research framework. *Communications of the Association for Information Systems*, 52, 293–331.<https://doi.org/10.17705/1CAIS.05214>
- 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>
- Calaza, T. (2024). Caught in the web: How e-commerce plays with consumer minds. *Brazilian Journal of Law, Technology and Innovation*, 2(2), 54–70.<https://doi.org/10.59224/bjlti.v2i2.54-70>
- Capone, V., Lo Presti, L., & Maggiore, G. (2025). Digital consumer vulnerability: A new theoretical framework through a systematic literature review. *Micro & Macro Marketing*, 2, 243–268.<https://doi.org/10.1431/114639>
- de Elizalde, F. (2025). Fragmenting consumer law through data protection and digital market regulations: The DMA, the DSA, the GDPR, and EU consumer law. *Journal of Consumer Policy*, 48(3), 355–389.<https://doi.org/10.1007/s10603-025-09584-3>
- Di Porto, F., & Egberts, A. (2024). The collective welfare dimension of dark patterns regulation. *European Law Journal*, 29(1–2), 114–141.<https://doi.org/10.1111/eulj.12478>
- Duivenvoorde, B., & Goanta, C. (2023). The regulation of digital advertising under the DSA: A critical assessment. *Computer Law & Security Review*, 51, 105870.<https://doi.org/10.1016/j.clsr.2023.105870>

- Durovic, M., & Poon, J. (2023). Consumer vulnerability, digital fairness, and the European rules on unfair contract terms: What can be learnt from the case law against TikTok and Meta? *Journal of Consumer Policy*, 46(4), 419–443. <https://doi.org/10.1007/s10603-023-09546-7>
- Fagan, P. (2024). Clicks and tricks: The dark art of online persuasion. *Current Opinion in Psychology*, 58, 101844. <https://doi.org/10.1016/j.copsyc.2024.101844>
- Fassiaux, S. (2023). Preserving consumer autonomy through European Union regulation of artificial intelligence: A long-term approach. *European Journal of Risk Regulation*, 14(4), 710–730. <https://doi.org/10.1017/err.2023.58>
- Hacker, P. (2023). The European AI liability directives: Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, 51, 105871. <https://doi.org/10.1016/j.clsr.2023.105871>
- Hair, J. F., Sarstedt, M., Ringle, C. M., Sharma, P. N., & Liengard, B. D. (2024). Going beyond the untold facts in PLS-SEM and moving forward. *European Journal of Marketing*, 58(13), 81–106. <https://doi.org/10.1108/EJM-08-2023-0645>
- Hayati, A. N. (2024). The issue of dark patterns in digital platforms: The challenge for Indonesia's consumer protection law. *Asian Journal of Law and Society*, 11(4), 453–465. <https://doi.org/10.1017/als.2024.24>
- Judijanto, L., Basri, T. S., Khulaili Harsya, R. M., Vandika, A. Y., & Utama, A. S. (2024). Kajian hukum dampak kecerdasan buatan terhadap perlindungan privasi data dalam hukum siber Indonesia. *Sanskara Hukum dan HAM*, 3(2), 68–76. <https://doi.org/10.58812/shh.v3i02.498>
- Khaerudin, A., Rosalia, O., Firayani, & Nasim, A. S. (2025). Responsibility of e-commerce platforms to consumers for illegal products in Indonesia. *Leges Privatae*, 1(5), 40–47. <https://doi.org/10.62872/ebwg8t95>
- Kim, K. K., 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>
- 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>
- Lechevalier, F., & Potel Saville, M. (2025). Fairness by design: Combatting deceptive AI-driven interfaces. *Cambridge Forum on AI: Law and Governance*, 1, e31. <https://doi.org/10.1017/cfl.2025.10018>
- Li, Y., Deng, X., Hu, X., & Liu, J. (2024). The effects of e-commerce recommendation system transparency on consumer trust: Exploring parallel multiple mediators and a moderator. *Journal of Theoretical and Applied Electronic Commerce Research*, 19(4), 2630–2649. <https://doi.org/10.3390/jtaer19040126>
- Liu, Y., & Sun, X. (2024). Towards more legitimate algorithms: A model of algorithmic ethical perception, legitimacy, and continuous usage intentions of e-commerce platforms. *Computers in Human Behavior*, 150, 108006. <https://doi.org/10.1016/j.chb.2023.108006>
- Maharani, R., & Prakoso, A. L. (2024). Perlindungan data pribadi konsumen oleh penyelenggara sistem elektronik dalam transaksi digital. *Jurnal USM Law Review*, 7(1), 333–347. <https://doi.org/10.26623/julr.v7i1.8705>
- Mende, M., Bradford, T. W., Roggeveen, A. L., Scott, M. L., & Zavala, M. (2024). Consumer vulnerability dynamics and marketing: Conceptual foundations and future research opportunities. *Journal of the Academy of Marketing Science*, 52, 1301–1322. <https://doi.org/10.1007/s11747-024-01039-4>
- Mourali, M., Novakowski, D., Pogacar, R., & Brigden, N. (2025). Post hoc explanations improve consumer responses to algorithmic decisions. *Journal of Business Research*, 186, 114981. <https://doi.org/10.1016/j.jbusres.2024.114981>

- Ning, X., Lu, Y., Li, W., & Gupta, S. (2024). How transparency affects algorithmic advice utilization: The mediating roles of trusting beliefs. *Decision Support Systems*, 183, 114273.<https://doi.org/10.1016/j.dss.2024.114273>
- Ostinelli, M., Bonezzi, A., & Lisjak, M. (2025). Unintended effects of algorithmic transparency: The mere prospect of an explanation can foster the illusion of understanding how an algorithm works. *Journal of Consumer Psychology*, 35(2), 203–219.<https://doi.org/10.1002/jcpy.1416>
- Park, K., & Yoon, H. Y. (2024). Beyond the code: The impact of AI algorithm transparency signaling on user trust and relational satisfaction. *Public Relations Review*, 50(5), 102507.<https://doi.org/10.1016/j.pubrev.2024.102507>
- Prihartanto, Y., Arifin, F., Maarif, I., & Kwarteng, A. H. (2025). From legal formalism to algorithmic justice: Rethinking consumer protection in the digital economy. *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, 14(1), 65–88.<https://doi.org/10.14421/gqmmwr98>
- Quinelato, P. D. (2024). Consumer manipulation through behavioral advertising: Regulatory proposal by the Data Services Act. *Brazilian Journal of Law, Technology and Innovation*, 2(1), 1–24.<https://doi.org/10.59224/bjlti.v2i1.1-24>
- Rott, P. (2025). Digital fairness and the burden of proof. *Journal of Consumer Policy*, 48(3), 297–314.<https://doi.org/10.1007/s10603-025-09583-4>
- Sa'adah, B. L. N., Sukarmi, & Dewantara, R. (2024). Establishing a personal data protection agency for e-commerce in Indonesia: Legal framework and implementation challenges. *Invest Journal of Sharia & Economic Law*, 4(2), 292–316.<https://doi.org/10.21154/invest.v4i2.10031>
- Schuett, J. (2024). Risk management in the Artificial Intelligence Act. *European Journal of Risk Regulation*, 15(2), 367–385.<https://doi.org/10.1017/err.2023.1>
- 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>
- Stewart, K., Perren, R., Chambers, C., & Zulauf, R. (2024). In tech we rely: How technology dependence fuels consumer vulnerability. *Journal of Consumer Affairs*, 58(4), 905–945.<https://doi.org/10.1111/joca.12610>
- Turillazzi, A., Taddeo, M., & Floridi, L. (2023). The digital services act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, 15(1), 83–106.<https://doi.org/10.1080/17579961.2023.2184136>
- Uceng, A., & Hanifah, A. M. Z. (2024). Dark patterns and consumer decision making in emerging markets: Experimental evidence from Indonesia. *Data: Journal of Information Systems and Management*, 2(3), 180–192.<https://doi.org/10.61978/data.v2i3.919>
- Waseem, D., Chen, S., Xia, Z., Rana, N. P., Potdar, B., & Tran, K. T. (2024). Consumer vulnerability: Understanding transparency and control in the online environment. *Internet Research*, 34(6), 1992–2030.<https://doi.org/10.1108/INTR-01-2023-0056>
- Witte, J., Kenning, P., & Brock, C. (2025). Dark patterns in online retailing: An analysis based on information manipulation theory. *European Journal of Marketing*, 59(13), 596–624.<https://doi.org/10.1108/EJM-04-2023-0302>
- Yulianingsih, S., & Putra, R. K. (2024). Analisis yuridis tentang perlindungan konsumen pada e-commerce di Indonesia: Pendekatan yuridis-normatif. *Hakim: Jurnal Ilmu Hukum dan Sosial*, 2(4), 842–856.<https://doi.org/10.51903/hakim.v2i4.2204>
- Zac, A., Huang, Y.-C., von Moltke, A., Decker, C., & Ezrachi, A. (2025). Dark patterns and consumer vulnerability. *Behavioural Public Policy*, 1–50.<https://doi.org/10.1017/bpp.2024.49>