



Gönderiliş Tarihi: 24/04/2026
Kabul Tarihi: 20/06/2026
ORCID 0000-0001-8561-8173

AI-BASED PERSONALIZATION AND CONSUMER TRUST: A CONCEPTUAL FRAMEWORK FOR UNDERSTANDING THE PERSONALIZATION–PRIVACY PARADOX

Bülent ŞEN¹

ABSTRACT

The rapid development of artificial intelligence has significantly transformed digital marketing practices, particularly through the widespread adoption of personalized customer experiences. While AI-based personalization enhances relevance, convenience, and decision efficiency, it simultaneously raises concerns about privacy, data usage, and algorithmic control. This duality is conceptualized in the literature as the personalization–privacy paradox. Drawing on existing literature, this study develops a comprehensive conceptual framework explaining how AI-based personalization influences consumer trust. The framework proposes that personalization generates two opposing perceptions-perceived benefit and perceived intrusiveness-which in turn shape trust. Trust functions as the central mechanism linking personalization to behavioral intentions, while algorithmic transparency and privacy assurance are introduced as moderating variables conditioning this relationship. By integrating previously fragmented research streams, the study offers a unified perspective on the dynamics between AI-based personalization and consumer trust, and argues that the impact of personalization on trust is highly conditional-dependent on the balance between perceived benefits and perceived privacy risks.

Keywords: Artificial Intelligence, Personalization, Consumer Trust, Privacy Concerns, Algorithmic Transparency

Jel Kodu: M31-D12-D18-D83

YAPAY ZEKÂ TABANLI KİŞİSELLEŞTİRME VE TÜKETİCİ GÜVENİ: KİŞİSELLEŞTİRME –GİZLİLİK PARADOKSUNA YÖNELİK KAVRAMSAL BİR ÇERÇEVE

ÖZ

Yapay zekâ teknolojilerindeki hızlı ilerleme, özellikle kişiselleştirilmiş müşteri deneyimlerinin yaygınlaşmasıyla birlikte dijital pazarlama uygulamalarını köklü biçimde dönüştürmüştür. Yapay zekâ tabanlı kişiselleştirme; uygunluk, kolaylık ve karar etkinliği bakımından tüketicilere belirgin kazanımlar sağlarken, gizlilik, veri kullanımı ve algoritmik kontrol konularında ciddi kaygıların da zeminini hazırlamaktadır. Bu ikili yapı, literatürde kişiselleştirme–gizlilik paradoksu olarak tanımlanmaktadır. Çalışma, mevcut literatüre dayanarak yapay zekâ tabanlı kişiselleştirmenin tüketici güveni üzerindeki etkisini açıklayan kapsamlı bir kavramsal çerçeve geliştirmektedir. Önerilen çerçevede kişiselleştirmenin iki zıt algı ürettiği ileri sürülmektedir: algılanan fayda ve algılanan müdahalecilik. Bu algılar, kişiselleştirme ile davranışsal niyetler arasındaki ilişkiyi aracıl原因 merkezi mekanizma olarak güveni şekillendirmektedir. Algoritmik şeffaflık ve gizlilik güvencesi ise söz konusu ilişkiyi koşullandıran düzenleyici değişkenler olarak modele dahil edilmiştir. Parçalı literatür akımlarını bütünleştiren çalışma, yapay zekâ tabanlı kişiselleştirme ile tüketici güveni arasındaki dinamiklere daha bütünlükçü bir bakış açısı kazandırmakta ve kişiselleştirmenin güven üzerindeki etkisinin koşullu olduğunu-algılanan fayda ile gizlilik riski arasındaki dengeye bağlı biçimde farklılaştığını-ortaya koymaktadır.

Anahtar Kelimeler: Yapay Zekâ, Kişiselleştirme, Tüketici Güveni, Gizlilik Kaygısı, Algoritmik Şeffaflık

Jel Codes: M31-D12-D18-D83

¹ Dr. Öğr. Üyesi, Tokat Gaziosmanpaşa Üniversitesi, Turhal Uygulamalı Bilimler Fakültesi, Elektronik Ticaret ve Yönetimi Bölümü, bulent.sen@gop.edu.tr

1. INTRODUCTION

The integration of artificial intelligence into marketing has fundamentally altered how firms interact with consumers. By enabling the analysis of large-scale consumer data, AI-driven systems make it possible to tailor content, recommendations, and communications at the individual level, thereby increasing the relevance and effectiveness of marketing activity (Jain et al., 2024; Arora et al., 2008). Through this transformation, personalization has moved well beyond its role as a supporting tool to become a central strategic mechanism in digital marketing.

From the consumer perspective, personalization is associated with lower information search costs, improved decision efficiency, and stronger perceived value. Empirical research has shown that personalization—particularly when it aligns with individual expectations and preferences—can increase engagement and reinforce trust (Bleier & Eisenbeiss, 2015; Kalaighnam et al., 2018). These benefits are not unconditional, however. The effectiveness of personalization depends not only on its functional value but also on how consumers interpret the collection and use of their personal data.

This tension is conceptualized in the literature as the personalization–privacy paradox—the coexistence of favorable attitudes toward personalized services and concerns about privacy and data usage (Xu et al., 2011; Awad & Krishnan, 2006). Consumers engage in a complex evaluation process in which perceived benefits are weighed against potential risks, a process further shaped by psychological factors such as perceived vulnerability, sense of control, and fairness (Dinev & Hart, 2006; Norberg et al., 2007).

How firms manage and communicate their data practices has a decisive influence on personalization outcomes. Transparency mechanisms and privacy assurances can reduce consumer uncertainty and favorably affect perceptions, whereas opaque or inadequate data practices may generate distrust and resistance (Lee & Cranage, 2011; Martin & Murphy, 2017). Personalization is therefore not merely a technological capability but a relational and ethical matter.

Consumer trust occupies a pivotal mediating role in this relationship. It determines whether consumers perceive personalization as beneficial or intrusive, and directly conditions their willingness to engage with digital platforms and share personal information (Gefen et al., 2003; McKnight et al., 2002). Research consistently shows that even the most sophisticated personalization strategies fail to deliver expected results when trust is absent (Bleier & Eisenbeiss, 2015).

The integration of AI into personalization systems adds further complexity. Predictive analytics, automated decision-making, and opaque algorithmic processes intensify privacy-related risks by fueling concerns about control, fairness, and data misuse (Menard & Bott, 2024; Goldfarb & Tucker, 2019). At the same time, AI technologies can enhance personalization accuracy and efficiency, creating a dual structure in which benefit and risk coexist rather than cancel each other out.

Research on consumer responses to AI-based systems underscores this complexity. While some individuals exhibit algorithm appreciation under certain conditions, algorithm aversion becomes more pronounced when errors or a lack of transparency are perceived (Logg et al., 2019; Dietvorst et al., 2015). This divergence suggests that trust in AI-driven personalization is jointly shaped by cognitive evaluations and emotional responses.

Despite a growing body of research on personalization, privacy, and trust, existing studies have examined these elements in fragmented and domain-specific ways. While several contributions address pairwise relationships, no framework integrates all three elements within an AI-specific context that simultaneously accounts for the dual-effect mechanism of personalization, the mediating role of trust, and the moderating functions of transparency and privacy assurance. Prior work either omits the AI dimension entirely, treats trust as a distal outcome rather than a central mediating mechanism, or examines transparency and privacy assurance as direct antecedents rather than boundary conditions. The present framework addresses precisely this configuration, which remains absent from the literature.

To address this gap, the study proposes a comprehensive conceptual framework explaining the relationship between AI-based personalization and consumer trust. It is argued that the effect of personalization on trust depends on the balance between perceived benefits and perceived privacy risks, and that this balance is conditioned by transparency, privacy assurance, and algorithmic characteristics.

2. CONCEPTUAL FOUNDATIONS OF AI-BASED PERSONALIZATION

2.1. The Structure and Dimensions of Personalization

AI-based personalization in digital marketing refers to a dynamic decision-making process grounded in machine learning algorithms, predictive analytics, and real-time data processing (Jain et al., 2024). Moving beyond traditional segmentation and rule-based targeting, this approach draws on multiple data sources—browsing history, purchase patterns, location data, and interaction behaviors—to produce highly individualized outputs. Through this capability, personalization has evolved from a static customization exercise into a continuous, automated, and self-improving process (Arora et al., 2008; Tam & Ho, 2006).

The conceptual structure of personalization revolves around three interconnected dimensions. Perceived relevance captures the degree to which personalized content aligns with consumers' needs and preferences; perceived benefit encompasses the functional gains derived from personalization, such as convenience and decision efficiency; and perceived intrusiveness reflects the extent to which personalization is experienced as invasive, excessive, or inappropriate (Bleier & Eisenbeiss, 2015). Together, these dimensions illustrate that personalization is evaluated not only by its technical accuracy but through subjective consumer perception.

2.2. AI's Contribution to Personalization-and the Complexity It Introduces

The integration of machine learning into personalization has substantially expanded both capability and complexity. Unlike traditional rule-based systems, which apply predefined criteria to segment consumers and deliver static content, machine learning-based personalization is dynamic: it infers latent preferences from behavioral signals, updates predictions in real time, and adapts recommendations without explicit human programming (Jain et al., 2024). This shift from legible rules to probabilistic inference has direct implications for consumer trust. When personalization logic is encoded in rules, consumers can plausibly understand why they receive certain content; when it is generated by predictive models, the basis of a recommendation becomes opaque even to the firms deploying the system. This opacity qualitatively changes the trust calculus, as consumers must evaluate not only the firm's intentions but also the reliability and fairness of a process they cannot observe (Menard & Bott, 2024).

A defining characteristic of AI-based personalization is that its algorithmic decision-making processes are often opaque to users. Unlike traditional systems, where personalization rules may be relatively legible, AI models frequently operate as black boxes: consumers find it difficult to understand how and why specific recommendations are generated. This opacity can adversely affect personalization perceptions, particularly when consumers cannot assess the fairness or accuracy of algorithmic outputs (Menard & Bott, 2024). For this reason, personalization must be understood not merely as a technological capability but as a socio-technical construct shaped by consumer perceptions, institutional practices, and the broader digital ecosystem (Goldfarb & Tucker, 2019).

Ethical considerations are therefore inseparable from the design of personalization systems. Personalization systems must preserve their functional value while also respecting user autonomy and privacy expectations, a balance that requires deliberate governance choices rather than purely technical optimization.

AI-based personalization represents a multidimensional construct that integrates technological, psychological, and ethical components. While it holds substantial potential for improving consumer experiences and firm performance, it simultaneously introduces new forms of complexity that shape how personalization is perceived and evaluated. Grasping these conceptual foundations is essential for the analysis of the relationship between personalization and consumer trust that forms the central focus of this study. Key studies bearing on this topic are summarized in Table 1.

Table 1. Key Studies on AI-Based Personalization, Privacy, and Consumer Trust

Author	Year	Context	Key Variables	Key Findings	Research Gap
Awad & Krishnan	2006	Online personalization	Privacy concern, data transparency,	Personalization creates value while simultaneously amplifying privacy concerns	AI context absent

				profiling willingness		
Dinev & Hart	2006	E-commerce	Privacy calculus, risk, behavioral intention	The benefit–risk trade-off is the primary determinant of consumer behavior	Algorithmic decision-making dimension absent	
Norberg et al.	2007	Consumer behavior	Privacy intention vs. actual behavior	A systematic gap exists between stated privacy concern and actual disclosure behavior	AI context absent	
Gefen et al.	2003	E-commerce trust	Trust, TAM, usage intention	Trust is the primary determinant of online purchase intention	Link to personalization not examined	
McKnight et al.	2002	Digital trust	Trust dimensions, e-commerce	Trust is multidimensional, encompassing cognitive and affective components	AI dimension absent	
Arora et al.	2008	One-to-one marketing	Personalization, customization, choice	Personalization effectiveness depends on the structure of consumer preferences	Privacy and trust dimension limited	
Tam & Ho	2006	Web personalization	Information processing, decision quality	Personalization improves decision efficiency and information processing outcomes	Trust and privacy dimension not examined	
Xu et al.	2011	Location-based marketing	Perceived benefit, risk, decision process	The personalization–privacy paradox is confirmed in a location-aware context	Trust mediation and AI integration weak	
Aguirre et al.	2015	Online advertising	Data collection mode, trust, ad effectiveness	Covert data collection markedly reduces trust compared to overt collection	AI and algorithmic personalization context absent	
Bleier & Eisenbeiss	2015	Online advertising	Trust, personalization sensitivity, ad effectiveness	Trust level is a key moderating variable that conditions personalization effectiveness	Intrusiveness and privacy concern dimension missing	
Kalaighnana m et al.	2018	E-commerce, retail	Web personalization, cash-flow volatility	Web personalization reduces cash-flow volatility and contributes to firm value	Consumer trust and privacy perception not examined	
Pan & Zinkhan	2006	Online privacy	Privacy disclosures, trust, online shopping	Privacy policy disclosures directly and positively influence consumer trust	Personalization and AI context absent	
Lee & Cranage	2011	Tourism and hospitality websites	Personalization, privacy assurance, consumer response	Privacy assurance reduces intrusiveness and facilitates positive consumer responses	AI and algorithmic context absent	
Martin & Murphy	2017	Data privacy and marketing	Privacy management, trust, marketing outcomes	How organizations manage personal data is a key determinant of consumer trust	AI and algorithmic processing dimension missing	
Goldfarb & Tucker	2019	Digital marketing	Privacy regulations, advertising effectiveness, data use	Privacy restrictions substantially constrain the effectiveness of digital advertising	Individual trust perception and personalization mechanism not examined	
Logg et al.	2019	Algorithm evaluation	Algorithm preference, human judgment, decision-making	Individuals can contextually prefer algorithmic judgment over human judgment	Privacy and personalization dimension absent	
Dietvorst et al.	2015	Algorithm evaluation	Algorithm aversion, error	Algorithmic error erodes trust more severely than equivalent human error	Marketing and personalization context not examined	

				perception, trust loss		
Menard Bott	&	2024	AI and privacy	AI misuse concern, information privacy	AI-specific misuse concern is validated as a construct distinct from general privacy concern	Behavioral intention and trust mechanism not modeled
Park Yoon	&	2024	AI transparency, public relations	Algorithmic transparency signal, trust, relational satisfaction	Explicitly communicating algorithm transparency increases user trust	Conditions under which transparency may heighten privacy concern not examined
Hu & Min		2025	AI robots, hospitality	Information transparency, privacy concern, behavioral intention	Increased transparency can raise data awareness and thereby amplify privacy concern	Integrated personalization–trust model not developed
Jain et al.		2024	AI and consumer behavior	AI applications, consumer response, research agendas	AI is fundamentally transforming consumer decision processes and marketing interactions	Trust and privacy integration model not developed
Kasap		2025a	E-commerce technology	Emerging technologies, AI applications, customer experience	AI-based tools are transforming e-commerce, though trust and privacy dimensions remain limited	Consumer trust and the personalization–privacy paradox not examined
Kasap		2025b	Industry 5.0, digital transformation	Human-centric AI, digitalization, societal transformation	Transition to human-centric, ethical AI systems is critically important in the Industry 5.0 era	Consumer-level trust and personalization analysis not conducted

Note: Table developed by the authors based on the reviewed literature.

3. CONSUMER TRUST IN DIGITAL ENVIRONMENTS

3.1. Structure and Components of Trust

Consumer trust is widely recognized as a foundational determinant of digital interaction, particularly in environments characterized by uncertainty, information asymmetry, and technological mediation. In online contexts where consumers cannot directly observe sellers, products, or processes, trust plays a decisive role in shaping behavioral intentions-including purchase decisions, information disclosure, and continued platform use (Gefen et al., 2003; McKnight et al., 2002).

Trust in digital environments is typically conceptualized as a multidimensional construct encompassing both cognitive and affective components. Cognitive trust is grounded in rational assessments of a system's competence, reliability, and functionality, while affective trust reflects emotional responses such as feelings of security, comfort, and perceived goodwill. This distinction is especially relevant in AI-based contexts, where consumers must evaluate not only the outputs of a system but also the processes through which those outputs are generated.

In the context of personalization, trust functions as the critical mechanism determining whether consumers interpret tailored experiences as beneficial or intrusive. When algorithmic recommendations are perceived as relevant, accurate, and supportive of decision-making, trust is reinforced; when personalization is experienced as excessive, manipulative, or invasive, it can give way to distrust. Findings showing that personalization effectiveness is largely contingent on pre-existing trust levels further support this reciprocal relationship (Bleier & Eisenbeiss, 2015).

3.2. The Role of Data Management and Privacy in Trust Formation

How personal data is perceived to be handled is a critical factor shaping trust in digital environments. Platforms that demonstrate transparency in data collection and use, and that offer credible privacy assurances, are more readily trusted by consumers. Privacy policy disclosures have been shown

to reduce uncertainty, strengthen perceived control, and thereby positively influence trust (Pan & Zinkhan, 2006). Broader research on data privacy similarly documents that trust is closely tied to how organizations manage, protect, and communicate personal information (Martin & Murphy, 2017).

Trust is shaped not only by privacy considerations but also by perceptions of fairness, control, and autonomy. When consumers feel they have limited control over their data-or that decisions are being made without their knowledge-trust can erode even in the presence of functional benefits. This dynamic is particularly pronounced in AI-based environments, where algorithmic decision-making processes are frequently opaque to users (Menard & Bott, 2024). Opacity creates uncertainty and can undermine trust even when outcomes appear accurate and useful.

3.3. How AI Reshapes Trust Dynamics

The growing use of AI technologies introduces new dimensions to trust formation. Unlike traditional digital systems, AI-based systems rely on automated inference and predictive analytics, which can amplify both trust and skepticism. On the one hand, they may be perceived as more objective and consistent than human decision-makers. On the other hand, concerns about algorithmic bias, errors, and misuse-especially when users cannot fully grasp how decisions are made-can seriously undermine trust (Goldfarb & Tucker, 2019).

Research on algorithmic decision-making illustrates the complexity of this picture. Some studies show that individuals can prefer algorithmic judgments under certain conditions, while others document that trust declines rapidly when algorithms err or appear unreliable (Logg et al., 2019; Dietvorst et al., 2015). These findings confirm that trust in AI systems is not static but shifts continuously in response to both performance and perception. Consumer trust in personalization thus emerges as a dynamic, multi-layered construct that reflects both the positive and negative effects of personalization. This dual character makes a clear examination of the conditions under which trust is reinforced or weakened both necessary and timely-and directs attention squarely to the personalization-privacy paradox.

4. THE PERSONALIZATION-PRIVACY PARADOX

4.1. Theoretical Foundations of the Paradox

The personalization-privacy paradox represents one of the most fundamental tensions in contemporary digital marketing, where data-driven and AI-enabled systems have become dominant. The paradox describes the coexistence of two apparently contradictory consumer responses: appreciation for personalized experiences and concern about the collection and use of personal data (Awad & Krishnan, 2006; Xu et al., 2011). Rather than reflecting inconsistency in consumer behavior, this coexistence points to a duality inherent in the personalization process itself.

Theoretically, the paradox can be explained through the logic of privacy calculus, whereby individuals evaluate personalized services by weighing perceived benefits against potential risks (Dinev & Hart, 2006). Personalization offers clear advantages-greater relevance, reduced search effort, improved decision efficiency-while simultaneously requiring the collection and processing of personal data, which can give rise to concerns about surveillance, misuse, and loss of control. These opposing forces operate concurrently, producing a dynamic evaluation process rather than a fixed outcome. The paradox does not settle at a universally stable equilibrium; it is context-dependent, varying with individual privacy sensitivity, prior experience, and situational conditions (Norberg et al., 2007).

How personal data is collected and used directly influences how the paradox manifests. When data collection is perceived as covert or opaque, consumers tend to respond more negatively-such practices heighten feelings of vulnerability and erode trust (Aguirre et al., 2015). When data practices are transparent and backed by trust-building mechanisms, consumers are more willing to accept personalization. These findings indicate that the paradox is conditioned not only by the existence of personalization but by the perceived legitimacy of the underlying processes.

4.2. How AI Intensifies the Paradox

The spread of AI-based personalization has deepened this paradox, as AI simultaneously expands both the capacity and the complexity of personalization systems. Firms can predict consumer preferences with increasing precision and deliver highly tailored experiences. Yet this capability rests

on extensive data extraction and algorithmic decision-making processes that consumers typically cannot understand or control (Menard & Bott, 2024). This dual expansion-in both capability and opacity-sharpens the tension between perceived benefit and perceived risk.

Algorithmic properties such as autonomy, adaptability, and opacity deepen this tension further. Because AI models continuously learn and evolve, their decision processes become less predictable from the user's perspective-increasing uncertainty and amplifying the sense of lost control, both of which are established antecedents of diminished trust. At the same time, rising personalization accuracy strengthens perceived benefit, producing a situation in which trust and concern coexist rather than displace one another. Perceived control is decisive in this equation: when consumers feel they have adequate control over their data, they are more likely to embrace personalization despite its risks; when control is perceived as absent, resistance can be triggered even where functional benefits are plainly evident.

Discussions of AI systems have brought to the fore a demand for technologies designed in alignment with ethical values and human well-being (Kasap, 2025b). From this vantage point, resolving the paradox is not merely a technical challenge but a normative one: personalization systems must be designed to benefit consumers while simultaneously protecting their autonomy and privacy.

5. ALGORITHMIC TRANSPARENCY AND ETHICAL CONCERNS

5.1. The Conditional Effect of Transparency on Trust

Algorithmic transparency refers to the degree to which users can understand how decisions are made within AI-based systems-how data are collected, processed, and transformed into personalized outputs. In digital marketing contexts, transparency may take the form of disclosing what types of data are used, explaining recommendation logic, or informing consumers why particular content is presented to them. Research supports the view that transparency reduces uncertainty and strengthens perceptions of system reliability, with corresponding positive effects on trust (Pan & Zinkhan, 2006; Park & Yoon, 2024).

The relationship between transparency and trust is not linear, however. While reducing ambiguity, transparency can simultaneously draw attention to data collection practices that consumers would otherwise have overlooked. Empirical evidence indicates that making algorithmic processes visible can fuel scrutiny and skepticism rather than confidence-particularly when consumers perceive inadequate safeguards or limited control (Hu & Min, 2025). Transparency is therefore insufficient on its own; it must be accompanied by meaningful privacy protections and credible assurances to function as a genuine trust-building mechanism. Perceived control plays a decisive role here: when users feel they have adequate command over their personal data and the personalization process, they are more willing to trust personalized services; when control is perceived as weak, personalization may be interpreted as intrusive or manipulative (Martin & Murphy, 2017).

5.2. Ethical Risks and Accountability

Ethical concerns surrounding AI-based personalization extend well beyond issues of transparency and control. Fairness, bias, accountability, and the responsible use of data have become focal points of ethical inquiry. AI systems can inadvertently reproduce or amplify biases embedded in training data, producing discriminatory or unfair outcomes. In personalization contexts-where algorithmic decisions directly shape consumer experiences, access to information, and access to opportunity-these risks are of particular significance.

The potential misuse of personal data constitutes an independent ethical concern. Menard and Bott (2024) validate AI misuse concern as a distinct construct: consumers' fears that their data will be used in unintended or unauthorized ways represent a form of privacy risk that differs from general privacy concern. These fears can substantially erode trust, especially when consumers lack clarity about how their personal information is managed or protected.

Digital platforms operate as complex ecosystems where personalization is integrated into large-scale data infrastructures. In this environment, trust is shaped not only by individual interactions but by perceptions of platform governance, corporate responsibility, and regulatory compliance. As transparency, accountability, and ethical responsibility become baseline expectations in the design and

deployment of algorithmic systems (Goldfarb & Tucker, 2019), the ethical design of personalization infrastructure emerges as a structural prerequisite for sustained consumer trust rather than a peripheral concern.

Algorithmic transparency and ethical concerns function as critical boundary conditions in AI-based personalization. Transparency can reduce uncertainty but may also heighten risk awareness; ethical safeguards can build trust but require credible implementation to do so. This dual character reinforces the need to position transparency and privacy assurance as moderating variables in understanding the relationship between personalization and consumer trust.

6. PROPOSED CONCEPTUAL FRAMEWORK AND HYPOTHESES

6.1. Structure of the Framework

Drawing on the existing literature, this study proposes an integrated conceptual framework explaining how AI-based personalization influences consumer trust and behavioral outcomes. Whereas prior research has largely treated personalization, privacy, and trust in isolation, the proposed framework brings these elements together in a unified structure that captures both the positive and negative effects of AI-driven personalization.

At the core of the model lies the premise that AI-based personalization simultaneously generates two opposing perceptions: perceived benefit and perceived intrusiveness. Perceived benefit reflects the degree to which consumers find personalization useful, relevant, and supportive of their decision-making. Perceived intrusiveness, by contrast, captures the extent to which personalization is experienced as invasive, excessive, or inappropriate. These two perceptions represent the primary mechanisms through which personalization is evaluated by consumers.

Perceived benefit is expected to have a positive effect on consumer trust. When personalization increases convenience, reduces information overload, and improves decision quality, consumers tend to regard the system as helpful and reliable-reinforcing trust in both the platform and its underlying technology (Bleier & Eisenbeiss, 2015). Perceived intrusiveness, conversely, is expected to exert a negative effect on trust. When personalization is associated with surveillance, loss of control, or inappropriate use of personal data, consumers may develop skepticism and distrust toward the system (Aguirre et al., 2015).

Consumer trust functions as the central mediating variable in the proposed framework. Trust is the bridge mechanism through which perceptions are translated into behavioral intentions-willingness to engage with the platform, share personal data, and make purchases. By reducing uncertainty and perceived risk, it facilitates positive behavioral outcomes in digital environments (Gefen et al., 2003). The decisive role that trust plays in linking both positive and negative perceptions to behavioral responses stands at the center of the model.

6.2. Moderating Variables: Transparency and Privacy Assurance

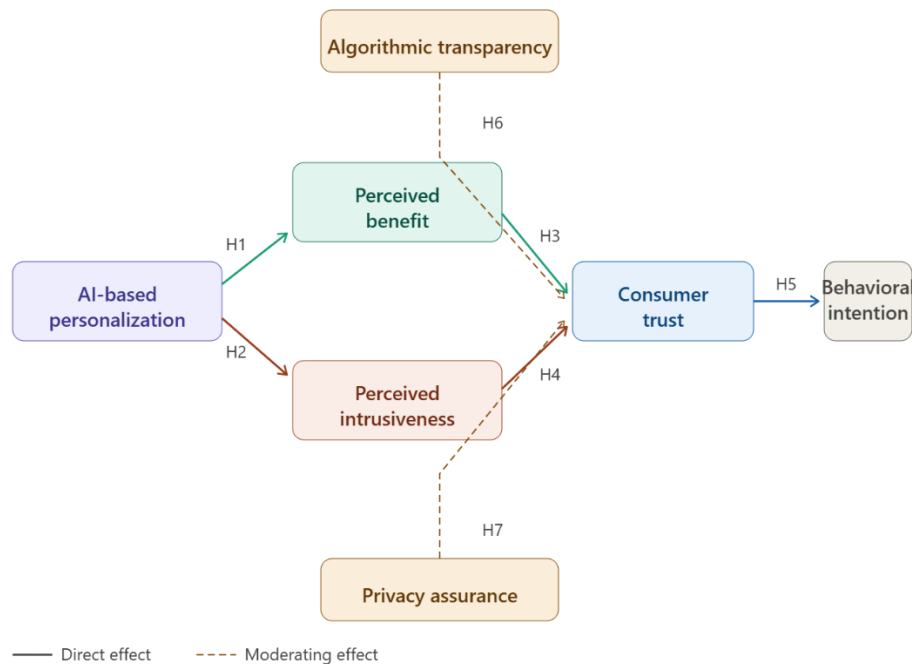
The framework also incorporates algorithmic transparency and privacy assurance as moderating variables that condition the relationship between personalization and trust. Algorithmic transparency refers to how well consumers understand how personalization decisions are made, while privacy assurance reflects the degree to which consumers believe their data are protected and used responsibly. These variables are included to capture the conditions under which personalization tends to generate trust rather than concern.

Algorithmic transparency is expected to weaken the negative effect of perceived intrusiveness on trust. When consumers are given adequate explanation of how personalization operates, they are more likely to perceive the system as legitimate and less threatening. Transparency may, however, also increase awareness of data practices, making its effect conditional rather than uniformly positive (Hu & Min, 2025). Privacy assurance is expected to strengthen the positive relationship between perceived benefit and trust by reinforcing consumers' sense of control and security over their personal information (Martin & Murphy, 2017).

The framework also accounts for the broader digital context in which AI-based personalization operates-one shaped by data-driven infrastructures, platform governance, and ethical considerations. In e-commerce environments, AI technologies improve customer experience while simultaneously raising

concerns about data privacy and system transparency (Kasap, 2025a). These contextual factors reinforce the need for a holistic approach to the personalization–trust relationship.

Figure 1. Proposed Conceptual Framework: AI-Based Personalization, Consumer Trust, and Behavioral Intention.



The framework presented in Figure 1 illustrates the proposed relationships among the core constructs. AI-based personalization operates as the exogenous variable, simultaneously activating perceived benefit and perceived intrusiveness as two opposing mediating pathways through which personalization shapes consumer trust. Consumer trust, positioned at the center of the model, translates these perceptions into behavioral intentions. Algorithmic transparency and privacy assurance function as moderating variables that condition the strength and direction of the intrusiveness–trust and benefit–trust relationships respectively, capturing the boundary conditions under which personalization is more or less likely to generate trust.

6.3. Proposed Hypotheses

Based on these theoretical considerations, the following hypotheses are proposed. H1 and H2 are grounded in Privacy Calculus Theory (Dinev & Hart, 2006), which holds that consumers simultaneously evaluate the utility and the risk of information-intensive services, implying that personalization activates both benefit perceptions and privacy-related concern. H3 and H4 follow from Social Exchange Theory, wherein trust is formed through repeated assessments of costs and benefits in relational exchanges: perceived benefit reinforces trust while perceived intrusiveness undermines it (Gefen et al., 2003). H5 draws on the established trust-behavior link in technology acceptance research, where trust reduces perceived risk and thereby facilitates engagement (McKnight et al., 2002). H6 is grounded in Signaling Theory: transparent disclosure of algorithmic logic functions as a credible signal of institutional competence and goodwill, reducing the ambiguity that amplifies intrusiveness perceptions (Park & Yoon, 2024). H7 builds on Privacy Calculus logic, with privacy assurance operating as a risk-reduction mechanism that strengthens the trust-generative capacity of perceived benefit (Martin & Murphy, 2017):

- H1:** AI-based personalization has a positive effect on perceived benefit.
- H2:** AI-based personalization has a positive effect on perceived intrusiveness.
- H3:** Perceived benefit positively influences consumer trust.
- H4:** Perceived intrusiveness negatively influences consumer trust.
- H5:** Consumer trust positively influences behavioral intention.

H6: Algorithmic transparency moderates the relationship between perceived intrusiveness and trust, such that higher transparency weakens the negative effect.

H7: Privacy assurance moderates the relationship between perceived benefit and trust, such that higher assurance strengthens the positive effect.

7. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

7.1. Theoretical Contributions

The primary theoretical contribution of this study lies in constructing an AI-specific integrative framework that reconfigures the roles of variables studied separately in prior work. While the personalization–privacy paradox, the benefit–intrusiveness duality, the mediating role of trust, and the governance functions of transparency and privacy assurance each have independent literatures, no prior model positions all four within a unified structure grounded in machine learning-based personalization that assigns trust an explicitly mediating rather than outcome role. The originality of the framework thus lies not in the novelty of individual constructs but in the theoretical configuration: the specific combination, the explicit causal ordering, and the AI-contextual grounding constitute a contribution that the constituent literatures, taken individually, do not provide. Against the assumption that personalization uniformly improves consumer experience, the proposed framework makes explicit that personalization simultaneously produces both perceived benefit and perceived intrusiveness, which helps explain why prior empirical research has generated conflicting results: personalization activates different perceptions concurrently, and how these perceptions are weighed varies across individuals, contexts, and system architectures.

Positioning consumer trust as a central mediating mechanism constitutes a further original contribution. Given that prior research has typically treated trust as an outcome variable, this study's characterization of trust as the critical link between consumer perceptions and behavioral intentions adds meaningful depth to the trust literature in algorithmic environments. Foregrounding the dynamic and context-sensitive nature of trust is central to this contribution.

The inclusion of algorithmic transparency and privacy assurance as moderating variables represents an additional dimension of the contribution. Existing studies have generally examined these factors in terms of direct effects. This study argues instead that their primary significance lies in conditioning the direction and strength of the relationship between personalization and trust. Transparency and privacy assurance are neither inherently beneficial nor inherently harmful; their effects depend on how they operate and what they are combined with.

Theoretically, the study extends the personalization–privacy paradox literature by introducing an AI-based perspective. Demonstrating that AI amplifies both the benefits and the risks associated with personalization is important for understanding how the paradox is evolving with technological advancement. The study also aligns with human-centric AI discussions that call for digital systems to be designed with user autonomy, fairness, and societal well-being in view—rather than efficiency alone.

7.2. Future Research Directions

Empirical validation of the proposed framework is the primary next step. While the theoretical foundations are sound, future research can employ methodological approaches such as structural equation modeling or experimental designs to examine how the proposed relationships operate in practice.

How individual differences shape responses to AI-based personalization is another important area for future inquiry. Privacy sensitivity, technological literacy, cultural background, and dispositional trust are among the factors that may significantly influence how consumers evaluate personalization. Incorporating these variables into the model could yield a more nuanced understanding of consumer behavior.

The context-specific nature of personalization also warrants deeper examination. Different sectors—e-commerce, social media, healthcare, and financial services—operate with distinct levels of perceived risk, trust expectations, and regulatory frameworks. Cross-sector comparative research could provide valuable insights into how contextual factors shape the personalization–trust relationship.

Beyond this, the effects of algorithmic design features-explainability, user control, and interface design-on perceptions of transparency and trust represent a promising avenue for bridging technical system design and consumer behavior research.

Operationalization of the proposed constructs is a further priority for future research. Perceived benefit and perceived intrusiveness can be measured through adapted scales from Bleier and Eisenbeiss (2015) and Aguirre et al. (2015) respectively, with items assessing relevance, convenience, invasiveness, and surveillance concerns. Consumer trust can be operationalized using the multidimensional scale of McKnight et al. (2002), distinguishing cognitive and affective components. Algorithmic transparency is measurable through items capturing comprehension of recommendation logic and perceived explainability, drawing on the scale validated by Park and Yoon (2024). Privacy assurance can be indexed via items reflecting perceived data protection, policy credibility, and user control, consistent with Martin and Murphy (2017). Behavioral intention is assessable through standard purchase intention and information disclosure willingness items. Researchers may also consider experimental manipulations of transparency level and privacy assurance condition to test H6 and H7 under controlled conditions.

8. LIMITATIONS

Several limitations of the proposed framework merit acknowledgment. First, as a conceptual rather than empirical contribution, the framework offers theoretical propositions rather than tested relationships; all causal claims remain tentative until validated through primary data. Second, the framework does not model the role of prior experience with personalized systems, which is established in the literature as a significant antecedent of both trust and privacy sensitivity. Third, cultural variation in privacy norms and trust dispositions is not captured; the framework is developed from a predominantly Western-centric literature and may require adaptation for collectivist or high-uncertainty-avoidance cultural contexts. Fourth, the model treats perceived benefit and perceived intrusiveness as independent dimensions, whereas empirical research suggests these may interact: very high benefit perceptions can suppress intrusiveness even at elevated data sensitivity levels, a dynamic not formally represented in the current structure. Fifth, the framework focuses on consumer-facing personalization and does not address organizational or B2B contexts where trust formation follows different logics. Future refinements should address these boundary conditions explicitly.

9. CONCLUSION

This study has proposed a comprehensive conceptual framework explaining how AI-based personalization influences consumer trust in digital environments. Integrating personalization research, privacy literature, and trust theory, the framework demonstrates that personalization is not a uniformly beneficial practice: it is a dual-effect mechanism that simultaneously generates perceived benefit and perceived intrusiveness.

Consumer trust plays a central role in translating these perceptions into behavioral outcomes. Perceived benefit can reinforce trust by enhancing relevance and decision efficiency; perceived intrusiveness can erode trust by deepening concerns about privacy, control, and data misuse. This dual character captures the essence of the personalization–privacy paradox, which becomes more pronounced in AI-based environments as algorithmic complexity and opacity increase.

The conditionality of personalization's effect on trust is a further key finding. Algorithmic transparency and privacy assurance are critical factors shaping how consumers interpret and evaluate personalization practices. These elements do not independently determine trust; rather, they influence the balance between benefit and risk, thereby conditioning whether personalization is perceived as supportive or intrusive.

By integrating previously fragmented research streams, this study offers greater clarity on the mechanisms underlying the effect of AI-based personalization on consumer trust. The future of AI-based personalization depends not only on technological advancement but equally on firms' capacity to design systems that are transparent, responsible, and user-centered. As digital environments continue to evolve, maintaining consumer trust will remain a fundamental priority.

REFERENCES

- Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34–49. <https://doi.org/10.1016/j.jretai.2014.09.005>
- Arora, N., Dreze, X., Ghose, A., Hess, J. D., Iyengar, R., Jing, B., Joshi, Y. V., Lurie, N. H., Neslin, S. A., Sajeesh, S., Su, M., & Syam, N. (2008). Putting one-to-one marketing to work: Personalization, customization, and choice. *Marketing Letters*, 19(3–4), 305–321. <https://doi.org/10.1007/s11002-008-9056-z>
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online. *MIS Quarterly*, 30(1), 13–28. <https://doi.org/10.2307/25148715>
- Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, 91(3), 390–409. <https://doi.org/10.1016/j.jretai.2015.04.001>
- Dietvorst, B. J., Simmons, J. P., & Massey, C. (2015). Algorithm aversion: People erroneously avoid algorithms after seeing them err. *Journal of Experimental Psychology: General*, 144(1), 114–126. <https://doi.org/10.1037/xge0000033>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90. <https://doi.org/10.2307/30036519>
- Goldfarb, A., & Tucker, C. (2019). Digital marketing and privacy. *Journal of Economic Literature*, 57(1), 3–43. <https://doi.org/10.1257/jel.20171452>
- Hu, Y., & Min, H. K. (2025). Information transparency, privacy concerns, and customers' behavioral intentions regarding AI-powered hospitality robots: A situational awareness perspective. *Journal of Hospitality and Tourism Management*, 63, 177–184. <https://doi.org/10.1016/j.jhtm.2025.04.003>
- Jain, V., Wadhvani, K., & Eastman, J. K. (2024). Artificial intelligence consumer behavior: A hybrid review and research agenda. *Journal of Consumer Behaviour*, 23(2), 676–697. <https://doi.org/10.1002/cb.2233>
- Kalaignanam, K., Kushwaha, T., & Rajavi, K. (2018). How does web personalization create value for online retailers? Lower cash flow volatility or enhanced cash flows. *Journal of Retailing*, 94(3), 265–279. <https://doi.org/10.1016/j.jretai.2018.05.001>
- Kasap, A. (2025a). E-commerce redefined: Harnessing emerging technologies for the future of trade. *International Journal of Economic and Administrative Academic Research*, 5(1), 54–79.
- Kasap, A. (2025b). Industry 5.0 and digitalizing societies: Turkey on the brink of a new revolution. *Uluslararası Anadolu Sosyal Bilimler Dergisi*, 9(1), 178–192. <https://doi.org/10.47525/ulasbid.1620668>
- Lee, C. H., & Cranage, D. A. (2011). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel web sites. *Tourism Management*, 32(5), 987–994. <https://doi.org/10.1016/j.tourman.2010.08.011>
- Logg, J. M., Minson, J. A., & Moore, D. A. (2019). Algorithm appreciation: People prefer algorithmic to human judgment. *Organizational Behavior and Human Decision Processes*, 151, 90–103. <https://doi.org/10.1016/j.obhdp.2018.12.005>
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. <https://doi.org/10.1007/s11747-016-0495-4>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>
- Menard, P., & Bott, G. J. (2024). Artificial intelligence misuse and concern for information privacy: New construct validation and future directions. *Information Systems Journal*, 35(1), 322–367. <https://doi.org/10.1111/isj.12544>
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100–126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, 82(4), 331–338. <https://doi.org/10.1016/j.jretai.2006.08.006>
- 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>
- Tam, K. Y., & Ho, S. Y. (2006). Understanding the impact of web personalization on user information processing and decision outcomes. *MIS Quarterly*, 30(4), 865–890. <https://doi.org/10.2307/25148757>
- Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1), 42–52. <https://doi.org/10.1016/j.dss.2010.11.017>