

Regulatory Compliance as a Critical Mediator Between AI Personalization and Consumer Loyalty on Digital Platforms.

الامتثال التنظيمي كوسيط حاسم بين تخصيص الذكاء الاصطناعي وولاء المستهلك في المنصات الرقمية

Soufyane Bouali ¹, Pradeep Mishra ², Selma Douha ³

¹ Setif 1 University Ferhat Abbas, Faculty of Economics, Business and Management Sciences – Setif (Algeria), soufyane.bouali@univ-setif.dz

² Department of Agricultural Statistics, College of Agriculture, JNKVV (Rewa, India), pradeepjnkvv@gmail.com

³ University of Batna 1, Faculty of Economics, Business and Management Sciences – Batna (Algeria), selma.douha@univ-batna.dz

Published: 26/01/2026

Accepted: 31/03/2026

Received: 31/03/2026¹

Abstract:

This study examines how AI-driven personalization on Indian e-commerce platforms like Flipkart impacts consumer trust and loyalty, within the framework of local data protection laws (IT Act 2000, SPDI Rules 2011). Using a quantitative survey of 520 users and Structural Equation Modeling (SEM), it tests a model where personalization and perceived privacy protection influence trust and loyalty. Key findings confirm that personalization strongly boosts both trust and loyalty. Crucially, perceived data privacy protection—shaped by regulatory compliance—not only directly strengthens trust and loyalty but also acts as a vital mediator. This means the positive impact of personalization on loyalty is significantly greater when users trust the platform's data governance. The results highlight that aligning AI innovation with transparent privacy practices is essential for building sustainable consumer relationships in regulated digital markets.

Keywords: AI-Driven Personalization, Data Privacy Protection, Consumer Trust, Platform Loyalty, Regulatory Compliance.

JEL Classification Codes: M31, L81, L86, O33

ملخص:

تناول هذه الدراسة أثر التخصيص القائم على الذكاء الاصطناعي في منصة التجارة الإلكترونية الهندية، (*Flipkart*)، على ثقة المستهلك وولائه، وذلك في إطار قوانين حماية البيانات المحلية واعتمدت الدراسة على مسح كمي شمل 520 مستخدماً، مع توظيف نمذجة المعادلات الهيكلية (*SEM*) لاختبار نموذج يوضح كيف يؤثر كل من التخصيص والإدراك المتعلق بحماية الخصوصية في الثقة والولاء. وتؤكد النتائج الرئيسة أن التخصيص يعزز بشكل قوي كلاً من ثقة المستهلك وولائه للمنصة. والأهم من ذلك، أن الإدراك المتعلق بحماية البيانات الشخصية والناجم عن الامتثال التنظيمي لا يسهم فقط بشكل مباشر في تعزيز الثقة والولاء، بل يعمل أيضاً كمتغير وسيط أساسي. ويعني ذلك أن الأثر الإيجابي للتخصيص على الولاء يكون أقوى بكثير عندما يثق المستخدمون في حوكمة البيانات التي تعتمدها المنصة. وتبرز النتائج أن مواءمة الابتكار القائم على الذكاء الاصطناعي مع ممارسات شفافة لحماية الخصوصية تُعدّ أمراً حاسماً لبناء علاقات مستدامة مع المستهلكين في الأسواق الرقمية الخاضعة للتنظيم.

كلمات مفتاحية: تخصيص، حماية البيانات الشخصية، ثقة المستهلك، ولاء، امتثال التنظيمي.

تصنيفات JEL: M31، L81، L86، O33

Corresponding author: Soufyane Bouali, e-mail: soufyane.bouali@univ-setif.dz

INTRODUCTION:

Research Introduction In the digital transformation era, consumption and trade patterns are fundamentally changing, as e-commerce platforms become a central hub of economic and social life. Within this context, artificial intelligence has emerged as a driving force in reshaping the consumer experience through intelligent personalization mechanisms that deliver content and recommendations tailored to individual preferences and digital behavior. However, technological progress is accompanied by profound governance challenges, ethical-legal dilemmas, particularly personal data protection and ensuring digital privacy. In India, a rapidly growing digital market, strict regulations are enforced under the Information Technology Act (IT Act 2000) and the Sensitive Personal Data or Information Rules (SPDI Rules 2011). This creates a critical testing ground for companies to find an appropriate balance between business innovation with legal compliance and societal trust. The research problem lies in the complex interplay between AI-driven personalization and digital trust loyalty construction under Indian legislation. The main research question raised by this study is: How can AI-based personalization achieve maximum commercial effectiveness toward loyalty and trust without conflicting with digital governance requirements and compliance with local laws? Subsidiary questions relate to consumer awareness about data protection mechanisms, how this affects their acceptance of personalized experience, and what role regulatory compliance plays—not as a technical obstacle but rather enabling factor for building sustainable relationships with users. This study has significant academic and practical importance because it fills a gap in the research literature that does not have empirical studies connecting applied AI systems with regulatory governance frameworks in emerging markets. It also theoretically contributes by integrating digital marketing models and trust theories with data governance frameworks to enrich scholarly discourse on managing emerging technologies. Practically, the study offers actionable insights for practitioners, policymakers, and digital platforms toward responsible legally compliant AI systems that enhance competitive advantage without undermining public trust. The main research objectives are:

1. To analyze the direct impact of perceived AI-driven personalization intensity on the Flipkart platform on consumer trust and platform loyalty.
2. To measure the impact of consumers' perception of their data privacy protection level on their trust and loyalty toward the platform.
3. To explore the potential mediating role of perceived privacy protection in the relationship between personalization and loyalty.
4. To identify the differences in the perception of privacy by demographic segments, particularly age categories.
5. To advance recommendations based on empirical evidence for improving the design of transparent, accountable AI systems corresponding to the Indian regulatory environment.

The study adopted an analytical quantitative research approach and collected primary data through a structured electronic questionnaire distributed among a sample of 520 active users of the Flipkart platform. Data analysis was carried out using a comprehensive set of statistical techniques involving Structural Equation Modeling (SEM) for model testing, multiple regression analysis for direct relationship testing, Sobel test and Bootstrap analysis for mediation effects validation, and one-way Analysis of Variance (ANOVA) for demographic differences. Measurement tools were developed and statistical software (SPSS and AMOS) was used to validate reliability and scientific credibility of results. Based on the extensive theoretical framework described earlier, the following research hypotheses are proposed:

(H1): There is a significant positive effect of perceived intensity of personalization on consumer trust in the platform.

(H2): There is a significant positive effect of perceived intensity of personalization on

Regulatory Compliance as a Critical Mediator Between AI Personalization and Consumer Loyalty on Digital Platforms

consumer loyalty toward the platform.

(H3): There is a significant positive effect of perceived data protection regarding privacy on consumer trust in the platform.

(H4): There is a significant positive effect of perceived data protection regarding privacy on consumer loyalty to the platform.

(H5): There is a significant positive effect of consumer trust toward loyalty to the platform.

(H6): Perceived data protection regarding privacy significantly mediates between perceived intensity of personalization and loyalty toward platforms.

(H7): Significant differences exist in terms of perceived data protection regarding privacy due to differences in users' age groups.

This research was based on a systematic review that covered several main themes: mechanisms for AI-driven personalization within e-commerce, frameworks for data governance and regulatory protection in India, digital trust concept along its dimensions, determinants for platform loyalty, as well as effects from demographic variables over perceptions about privacy. The gap revealed by this review was one wherein very few studies had attempted to connect all these aspects within any specific regulatory context such as that of India; hence it was decided to undertake this study.

The key operational terms used in this study are defined as follows:

- Artificial Intelligence-Driven Personalization: A computer system that provides recommendations and content based on machine learning algorithms and data mining techniques that automatically and dynamically adapt to the user's preferences by analyzing their behavior.
- Perceived Data Privacy Protection: The user's perception of how much the platform complies with regulatory and legal requirements in terms of collecting, storing, processing, and deleting personal data by observing whether informed consent, data minimization, and limited retention are practiced.
- Trust in Digital Platform: The psychological state of a user trusting the technical competence (competence), integrity (integrity), and benevolence of a digital platform.
- Loyalty Toward Platform: An enduring behavioral and emotional commitment toward repurchase, resistance to switching alternatives, and positive word-of-mouth recommending this platform to others.
- Indian Regulatory Framework: It consists of the Information Technology Act 2000 as amended from time to time and Sensitive Personal Data or Information Rules 2011 along with the obligations prescribed thereunder for data processing

2. Literature Review

The fast growth of online shopping has come with more and more use of systems controlled by AI to make experiences better for customers, keep them engaged (Bag, 2022), and improve how businesses run. Making things personal means changing content, product ideas, search results, and advertising offers for each user based on their history of browsing, buying habits, and other actions data (Theodorakopoulos, 2024). Websites like Flipkart get anonymous session data such as views on products added to carts checkouts purchases in order to build real-time personalization without linking recommendations to identifiable personal information. These practices of collecting and keeping data are directly related to India's IT Act 2000 and SPDI Rules 2011 that require explicit consent before collecting any data; minimal necessary collection of personal and sensitive data; disclosure of processing practices; retention within defined time periods. For example, Flipkart has a policy about keeping user-eye-tracking data for one month and session data for two months which matches with the idea of limited retention under SPDI Rules, thus lowering possible regulatory and

reputation risks.

2.1. AI-Driven Personalization in E-Commerce

AI-driven personalization makes use of advanced algorithms such as collaborative filtering, content-based filtering, and hybrid approaches to predict user preferences, optimize recommendations, and enhance the overall shopping experience. These algorithms analyze patterns of user behavior, transaction histories, search queries, browsing time, and clickstream data in order to generate product suggestions that are tailored to individual interests. The effectiveness of these systems depends on the quality, granularity, and timeliness of behavioral data as well as the integration of cross-channel touchpoints across mobile apps, websites, and email campaigns (Lund, 2021). AI-driven personalization is perceived to improve convenience, satisfaction, and engagement; it can also strengthen brand loyalty by fostering a sense of individualized attention and recognition. Research indicates that consumers are more likely to return to platforms that provide consistent and relevant recommendations since positive experiences enhance long-term brand equity and word-of-mouth advocacy (Lamarre, 2023).

But collecting too much personal data can lead to legal issues, ethical concerns, and damage the company's reputation. In India, the Information Technology (IT) Act 2000 and SPDI Rules 2011 require companies to get explicit consent from users before they can collect sensitive personal data. They also need to inform users about how long they will keep this data. If companies do not follow these rules, they risk losing user trust and legitimacy in real-time personalization systems where large datasets are processed continuously while predictive models adapt dynamically to user behavior (Mohammadi, 2019). Ethical concerns also emerge around algorithmic bias autonomy fairness AI models trained on historical data may inadvertently reinforce stereotypes or preferential treatment affecting user perceptions of fairness additionally transparency challenges arise when the personalization process is perceived as a “black box” leaving consumers uncertain about how their data is used and what drives recommendations (Choudhary, 2023). To mitigate these risks firms are encouraged to adopt privacy-by-design principles provide clear opt-in and opt-out mechanisms communicate recommendation logic in accessible formats.

2.2. Data Protection and Governance in Tailored E-Commerce

Data protection is the foundation of consumer trust in AI-based personalization in e-commerce. The perceived protection of data encompasses the beliefs of consumers about how a platform responsibly collects, stores, processes, and shares personal information. Compliance with India's SPDI Rules (Jayapal, 2025) and the IT Act (2000) is critical as these frameworks require prior informed consent, disclosure about the purpose for which data is being collected, retention policy information, and access protocols. Platforms that use privacy-preserving techniques such as anonymization, data minimization, pseudonymization, and role-based access control are seen as more trustworthy (Saxena, 2023). For instance, Flipkart has data governance mechanisms whereby product recommendations are de-linked from user identifiers; sensitive personal information is not stored and if it is then it will be encrypted; operational practices comply with legal requirements as well as best practices in user-centric privacy. In the same way Tata Neu focuses on selective retention of data and transparent consent mechanisms across its super-app ecosystem to give signals of integrity to consumers while enabling personalization at scale (Kavitha, 2023).

Regulatory Compliance as a Critical Mediator Between AI Personalization and Consumer Loyalty on Digital Platforms

Evidence from empirical studies shows that users' perception of strong privacy governance plays a mediating role between trust and loyalty toward the platform, thus underscoring the strategic significance of regulatory compliance with AI personalization strategies (Jayapal, J., 2025). Furthermore, platforms that communicate their privacy safeguards proactively—and take responsibility for their algorithmic decision-making—are more likely to reduce perceived risk foster engagement and build long-term loyalty.

2.3. Consumer Trust in Digital Platforms

Trust is a key relational construct in online consumer behavior that reduces perceived risk and uncertainty facilitating the adoption of AI-driven personalization. Three important dimensions of trust have been identified in research: competence, benevolence, and integrity which are affected by personalization as well as privacy practices (Anwar, 2021). In India, compliance with IT Act provisions and SPDI Rules enhances trust through secure data storage, obtaining explicit consent for processing for specific purposes along with disclosures regarding the use of data indicating organizational integrity and reliability. If personalization is viewed as opaque or non-compliant then it can quickly erode trust resulting in decreased engagement increased churn and lower brand loyalty (Lakasing, 2025). Examples like Zomato and Ola show that privacy-conscious algorithmic design coupled with overt compliance can maintain user trust even when dynamic pricing or real-time AI recommendations are applied; this mitigates skepticism about the misuse of personal data.

Moreover, trust also serves as a mediating mechanism between the intensity of perceived personalization and the resulting behavioral outcomes. Users are likely to follow recommendations and interact with them multiple times if they perceive both technical competence and ethical integrity in how the platform operates.

2.4. Loyalty Toward the Platform and Its Results

Platform loyalty includes attitudinal commitment and behavioral engagement, such as repeated purchases, continued use, and advocacy behaviors. AI-driven personalization increases loyalty by increasing perceived convenience, relevance, and satisfaction; thus creating a feeling of individualized attention that strengthens emotional bonds with the brand (Bilgihan, 2025). Regulatory compliance is important for reinforcing loyalty. Under SPDI Rules, users expect full disclosure on data collection details, retention period, and sharing policy (Morgan G. &, 2018). Platforms that do not meet these expectations will undermine loyalty even if personalization works from an operational viewpoint (Clauss, 2019). On the other hand, strong privacy and governance practices are used as strategic tools rather than just legal compliance to let firms differentiate themselves in competitive e-commerce markets (Jamal, 2003). For example, Flipkart's super-app ecosystem and Tata Neu deploy privacy-by-design as well as purpose-limited personalization that results in higher repeat purchase rates with lower churn accompanied by better customer advocacy. Session frequency, basket size, and recommendation conversion rates are all behavioral metrics that can directly connect to trust perceptions derived from transparent data governance.

2.5 Variation Across Demographics and Their Perception About Privacy

Demographics of consumers play an important role in how personalization is viewed along with governance practices. It has been found that older users, those having lower digital literacy levels, and segments who value privacy highly become more sensitive to risks related

to it; thus they may respond negatively toward perceived overreach in data collection (Galvez-Cruz, 2009). In India SPDI Rules require explicit consent plus disclosure obligations plus retention limits which help reduce demographic disparity through equitable awareness raising about control over one's personal information. Studies show compliance with these measures reduces heterogeneity in privacy perceptions resulting in consistent trust and loyalty across diverse user segments including urban/rural population spread over different age groups/income levels. Byju's and Ola (Prasanna, 2025, November) have created different consent interfaces along with varying privacy notifications based on demographic diversity so that personalization remains inclusive as well as transparent/culturally sensitive thereby reducing the risk of alienating vulnerable less tech-savvy users.

2.6. Gaps in the Literature

While numerous studies have been conducted on AI-enabled personalization, trust, and loyalty, several significant gaps still exist within the Indian e-commerce context: Cross-border data flows and their interaction with India's emerging data localization policies have been underexplored. Limited research exists regarding consumer awareness, agency, and behavioral responses to AI recommendations as well as consent mechanisms. Perceived data privacy protection has not been sufficiently investigated in terms of its mediating role between personalization and loyalty. Algorithmic governance practices such as auditing, bias mitigation, ethical AI design, and regulatory compliance have received little attention from researchers. The impact of dynamic personalization in real-time environments—for example surge pricing or context-driven recommendations—on consumer trust and loyalty remains largely unstudied in Indian settings. These gaps need to be filled in order to create evidence-based frameworks for ethical, compliant, and effective AI personalization on Indian e-commerce platforms.

The conceptual framework incorporates compliance with the Indian IT Act and SPDI Rules through consent management, purpose limitation, retention periods, access restrictions, and security safeguards. This ensures that both commercial objectives and governance responsibilities are addressed systematically. Such a dual focus would align technological innovation with ethical imperatives as well as legal necessities—positioning AI-driven personalization not only as a means for enhancing consumer experience but also one that preserves trust while supporting long-term brand loyalty.

3. Hypotheses Development

AI-powered personalization is a key strategic capability of e-commerce platforms that allows firms to provide highly personalized product recommendations, search results, and content based on individual user preferences, past behaviors, and browsing history. Personalization is not just a means to improve user experience but also a critical tool for maintaining competitive advantage in ever more crowded digital marketplaces. Prior research shows how personalization enhances perceived convenience, relevance, and satisfaction which subsequently affect consumer behavioral outcomes such as trust, loyalty, and purchase frequency (Komiak, 2006). The effectiveness of AI-powered personalization depends on user perceptions regarding the responsible and transparent management of their data; thus highlighting the nexus between commercial performance and governance considerations particularly concerning the Indian IT Act 2000 and SPDI Rules 2011 that govern consent purpose limitation as well as data protection practices.

Regulatory Compliance as a Critical Mediator Between AI Personalization and Consumer Loyalty on Digital Platforms

Perceived intensity of personalization is the extent to which users perceive that interactions with the platform—recommendations, search results, content—are tailored specifically to their preferences and needs. Personalization is an effective signal of how capable, caring, and responsive a platform is which reduces uncertainty for users thereby instilling confidence in it. Theoretical frameworks from marketing and information systems research indicate that such positive signals help establish cognitive trust as well as affective trust thus creating an emotional bond between consumer and platform (Lee, 2015). This leads us to hypothesize that perceived intensity of personalization has a positive significant effect on consumer trust towards Flipkart (H1). It also indicates that AI-driven personalization can function both as a technological mechanism as well as a relational mechanism for enhancing trust.

Apart from trust formation, personalized interactions are expected to have a direct impact on platform loyalty by increasing perceived value convenience relevance of the shopping experience. Personalization increases the likelihood of repeat purchases long-term engagement through streamlining decision-making reducing cognitive load providing targeted recommendations. These sustained interactions according to relationship marketing theory result in behavioral attitudinal loyalty implying that consumers increase their commitment towards the platform based on positive experiences repeated (Thaichon, 2020). Thus perceived intensity of personalization is hypothesized to positively significantly impact platform loyalty (H2) reflecting direct commercial benefits derived from algorithmic personalization.

Trust in digital platforms goes beyond just perceived quality of service to perceived responsible data governance. Consumers are now increasingly aware of the data privacy risks that come with AI systems and those platforms that are perceived as secure and transparent in their data collection and usage practices will elicit trust more readily. This is particularly applicable in India, where the SPDI Rules mandate explicit consent, purpose limitation, and disclosure of data processing practices. Users who feel that their personal information is well protected would view Flipkart as a trustworthy and ethical platform. Hence it can be hypothesized that perceived data privacy protection positively and significantly affects consumer trust in Flipkart (H3). This hypothesis combines both behavioral and governance perspectives by showing how compliance with regulations as well as assurance of privacy help create trust. Perceived data privacy protection will also have a direct impact on platform loyalty apart from its impact on trust. Privacy assurance lessens the perceived risk of repeated online interactions and reduces the uncertainty regarding the management of personal data. Therefore, users who feel that strong data protection is in place are more likely to stay engaged with the platform for a longer period of time while also showing greater loyalty intentions, thus supporting our hypothesis that perceived data privacy protection positively and significantly affects platform loyalty (H4). This direct link underlines how commercially valuable it is to comply with privacy regulations as well as to govern beyond mere compliance by aligning legal adherence with user-centered outcomes.

Consumer trust is a vital relational mechanism linking platform capabilities to sustained loyalty and engagement. Trust-commitment theoretical models show that higher levels of trust reduce perceived relational risk and increase consumers' willingness to continue using the platform, recommend it to others, and transact repeatedly (Morgan R. M., 1994). Thus, we

hypothesize that consumer trust has a positive and significant effect on platform loyalty (H5). The pathway illustrates interdependence between technology-mediated personalization, governance practices, and attitudinal outcomes.

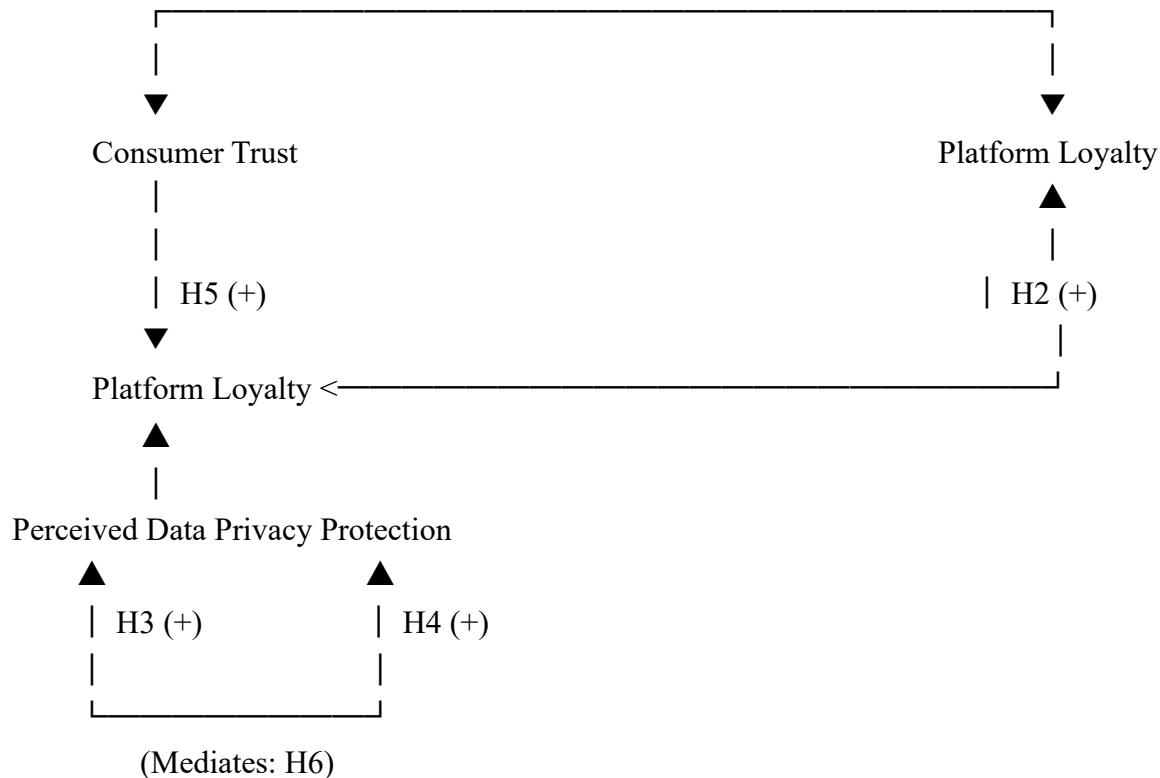
Although personalization can enhance loyalty directly, its effect may be moderated or mediated by users' perceptions of privacy protection. Excessive, opaque, or intrusive personalization may raise privacy concerns and erode trust to the extent that it does not enhance loyalty outcomes. Mediation theory suggests that perceived data privacy protection is a filter that determines the degree to which personalization translates into sustained loyalty. It is therefore hypothesized that perceived data privacy protection mediates the relationship between perceived personalization intensity and platform loyalty (H6). This hypothesis is an integration of technological, behavioral, and regulatory dimensions in the complex dynamics of AI-driven personalization in regulated e-commerce environments.

Demographic characteristics such as age, experience, and digital literacy affect how users perceive and interpret personalization as well as data governance practices. Previous studies have shown that older users and those who are less digitally experienced tend to be more sensitive to privacy issues and scrutinize platform practices more closely (Acquisti, 2020). In this setting, perceived data privacy protection is expected to vary considerably across age groups since it embodies heterogeneity in governance expectations and risk perceptions. Therefore, it is hypothesized that perceived data privacy protection varies significantly across age groups (H7).

These seven hypotheses together form an integrated conceptual framework capturing the value-creation role of AI-driven personalization with governance mechanisms shaping trust and loyalty. The framework will be empirically tested using regression analysis, structural equation modeling, mediation analysis, and group comparison techniques for a complete understanding of how AI personalization interacts with user perceptions, regulatory compliance, and behavioral outcomes in the Indian e-commerce context.

Regulatory Compliance as a Critical Mediator Between AI Personalization and Consumer Loyalty on Digital Platforms

Fig (1): Research Hypotheses Summary
Perceived Personalization Intensity



Demographic Variable: Age Groups ———▶ Perceived Data Privacy Protection (H7)

Source: Authors' elaboration

The study's conceptual framework is depicted in Figure 1, which also highlights the connections between platform loyalty, consumer trust, perceived data privacy protection, and perceived personalization intensity. The figure illustrates how personalization directly affects trust and loyalty (H1–H2), how data privacy protection influences trust and loyalty (H3–H4), how privacy protection mediates the relationship between personalization and loyalty (H6), how trust affects loyalty (H5), and how privacy perception varies by demographic (H7). This framework offers a clear path for empirical testing by integrating governance and commercial viewpoints.

4. Methodology

4.1. Research Design

This study follows a quantitative, explanatory research design to study the relationships among AI-driven personalization, perceived data privacy protection, consumer trust, and platform loyalty in Flipkart's e-commerce environment. A cross-sectional survey approach was used to capture users' perceptions at one time which is suitable for studying attitudinal and behavioral outcomes related to algorithmic personalization. The research design is based on a positivist paradigm that focuses on hypothesis testing and empirical validation of theorized relationships. Flipkart was chosen as a single in-depth case study because it has advanced personalization infrastructure, a large diverse user base, and operates within India's evolving data protection and governance framework. This case-based quantitative design enables contextualized empirical insights while keeping analytical rigor intact. The conceptual

model identifies perceived personalization intensity as the main independent variable, trust and platform loyalty as dependent variables, and perceived data privacy protection as a mediating construct. Demographic and usage-related variables were included as controls to account for heterogeneity in user characteristics and engagement patterns.

4.2. Data Analysis Techniques

Data analysis was done through a multi-stage statistical approach to ensure robustness and methodological transparency. First, descriptive statistics were computed to summarize sample characteristics by assessing central tendencies and dispersion across key constructs. Reliability analysis was performed using Cronbach's alpha and composite reliability (CR) for internal consistency evaluation. Second, correlation analysis (Pearson's r) was applied for bivariate relationships so that initial support could be provided for the hypothesized associations between variables. Direct effect testing used multiple linear regression analysis with multicollinearity diagnostics conducted via Variance Inflation Factors (VIF) for model stability checks. Third, structural equation modeling (SEM) estimated measurement models simultaneously with structural models allowing assessment of construct validity and overall model fit; χ^2/df CFI TLI RMSEA SRMR were established fit indices used in evaluating model adequacy Convergent validity was assessed through Average Variance Extracted (AVE) discriminant validity through inter-construct correlations Fourth, the mediating role of perceived data privacy protection was examined using both bootstrapped indirect effects and the Sobel test enabling robust inference regarding mediation pathways Effect sizes Cohen's f^2 predictive relevance Stone–Geisser's Q^2 values.

Lastly, one-way ANOVA was run to assess demographic variations especially across the age categories in privacy perception and thereby provide further insight into heterogeneity in governance expectations. It was assumed that all statistical analyses would be performed using software packages like SPSS and AMOS, with a significance level of $p < 0.05$.

The methodology merges conventional statistical methods with advanced modeling techniques to capture both behavioral and governance-related dynamics of AI-driven personalization. By integrating regression analysis, SEM, and mediation testing, this study presents an all-encompassing analytical framework that is well-suited for exploring challenges related to AI governance in new e-commerce market environments.

5. Results and Analysis

This study uses a dataset from a quantitative survey that aimed to explore the implications of governance, privacy, and trust in AI-driven personalization on Flipkart's e-commerce platform. The dataset contains valid observations from 520 active Flipkart users who had made at least one purchase in the last six months. This criterion was necessary to ensure that respondents had enough exposure to the personalized recommendation and search features of the platform for forming valid perceptions. The dataset consists of four categories of variables. First, demographic variables identify the gender and age group of respondents. Second, usage-related variables capture access mode (mobile application versus website) and purchase frequency (repeat versus occasional purchases). Third are perceptual constructs that measure perceived intensity of personalization, perceived data privacy protection, trust in Flipkart, and loyalty to the platform. Lastly, control variables include overall usage intensity and familiarity with online shopping platforms. All perceptual constructs were measured using multi-item scales on a five-point Likert scale ranging from 1 ("strongly disagree") to 5 ("strongly agree"). Measurement items were taken from well-known studies related to digital personalization, consumer trust, and data privacy but reworded contextually for Flipkart's AI-

Regulatory Compliance as a Critical Mediator Between AI Personalization and Consumer Loyalty on Digital Platforms

driven personalization environment. Internal consistency reliability was established through Cronbach's alpha and composite reliability scores which were above the recommended thresholds. The survey was conducted through an online medium over a period of three months using a structured self-administered questionnaire. It was assumed that distribution happened by digital channels popular among Indian e-commerce consumers, such as email invitations and in-app survey prompts. Participation was on a voluntary basis without collecting any personally identifiable information. Before starting the survey, respondents were shown an informed consent statement that clearly described the purpose of the study, what kind of data would be collected, and their rights as participants. Respondents were assured that all responses would be anonymized and aggregated for academic research purposes only following principles similar to those found in India's IT Act and SPDI Rules. To improve data quality, incomplete responses as well as questionnaires showing straight-lining or inconsistencies were removed from the final dataset; this left a clean sample of 520 usable responses. Descriptive and inferential analyses followed standard statistical techniques such as correlation analysis regression modeling structural equation modeling. Though the dataset does not contain sensitive personal data as defined under the SPDI Rules, the survey design complies with best-practice data governance principles such as data minimization, purpose limitation, and transparency. It was assumed that reasonable security practices would be used for data storage and processing, with access restricted to those needed and retention limited to what was required for the study. This structured dataset and mode of administration support methodological rigor through internal consistency, construct validity, and analytical robustness. The structure of this dataset allows direct and mediated relationships among personalization, privacy perception, trust, and loyalty to be examined while still being in line with current regulatory and governance expectations within an Indian e-commerce context.

Table (1): Demographic and Usage Profile of Respondents (N = 520)

Variable	Category	Frequency	Percentage (%)
Gender	Male	281	54.0
	Female	239	46.0
Age	Under 25 years	86	16.5
	25–40 years	322	61.9
	Above 40 years	112	21.6
Usage Type	Mobile application	333	64.0
	Website	187	36.0
Purchase Frequency	Repeat purchases	369	71.0
	Occasional purchases	151	29.0

Source: Authors' elaboration

The demographic and usage profile shows a balanced and commercially relevant sample, very well aligned with Flipkart's core user base. 54% male and 46% female near-equal gender distribution reduces gender bias and increases generalizability across diverse consumer segments. Age-wise, the high percentage of users between 25-40 years old (61.9%) reflects most economically active and digitally literate cohort that is usually more open to AI-driven personalization features. This group also has an increased probability of frequent online transactions, making it particularly relevant for assessing trust and loyalty outcomes. At the same time, the presence of users above 40 years old (21.6%) ensures that privacy sensitivity differences can be meaningfully captured, as will be discussed in ANOVA results later on.

The usage-type distribution indicates a strong preference for the mobile application (64%), which is also consistent with other reports on Indian e-commerce consumption patterns. This has significant governance implications since mobile environments typically mean continuous data capture, location-based signals, and device identifiers are all at play; hence there is much greater need for transparent consent as well as session-level data controls to comply with SPDI Rules. The high proportion of repeat purchasers (71%) indicates that this sample mostly comprises experienced users who have been repeatedly exposed to Flipkart's personalization mechanisms. This increases the validity of inferences relating to trust formation and loyalty since perceptions are based on long-term interaction rather than just one-off transactions.

Table (2): Descriptive Statistics of Key Study Constructs

Construct	Mean	Standard Deviation
Perceived Personalization Intensity	4.12	0.68
Perceived Data Privacy Protection	3.46	0.74
Trust in Flipkart	3.98	0.71
Platform Loyalty	4.05	0.66
<i>Measured on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree).</i>		

Source: Authors, PLS (2025V)

The descriptive statistics show a clear ranking between user perceptions and provide key information about the interaction of AI-driven personalization at Flipkart.

Perceived personalization intensity has the highest mean value ($M = 4.12$), which implies that users strongly perceive and feel the personalized features of the platform in all aspects of their browsing and purchasing journey. This indicates that Flipkart's recommendation, search ranking, and content personalization systems are both highly visible and efficient from the perspective of users. Trust in Flipkart ($M = 3.98$) and platform loyalty ($M = 4.05$) also have relatively high mean scores to reflect favorable attitudinal and behavioral outcomes associated with long-term exposure to personalization. The relatively low standard deviations for these constructs indicate consistent perceptions among respondents, thereby reinforcing the reliability of findings. On the other hand, perceived data privacy protection has a much lower mean ($M=3.46$) with the highest standard deviation ($SD=0.74$). This pattern indicates more heterogeneity in privacy perceptions, which means that there is uncertainty or ambivalence among users about how their data are being collected, processed, and protected. Even though Flipkart complies with existing regulatory requirements, users seem less confident about privacy protections than they are about personalization benefits. From a governance point of view, such differences between high personalization and relatively lower privacy perception indicate a crucial compliance perception gap. AI-driven personalization works well to build trust and loyalty; however, this finding suggests that legal compliance does not necessarily convert into perceived privacy assurance.

Such a gap becomes particularly relevant under the Indian IT Act and SPDI Rules because these laws stress informed consent, purpose limitation, and transparency. Results hint at strengthening user-facing transparency mechanisms—like simplified privacy explanations and contextual consent prompts—as essential to align regulatory compliance with user expectations.

Table (3): Effect Size (Cohen's f^2)

Relationship	R^2 (Before)	R^2 (After)	f^2	Effect Size Interpretation
Personalization → Trust	0.19	0.43	0.42	Large effect
Personalization → Loyalty	0.21	0.34	0.35	Large effect
Privacy Perception → Loyalty	0.34	0.47	0.25	Medium effect

Source: Authors, PLS (2025V)

Regulatory Compliance as a Critical Mediator Between AI Personalization and Consumer Loyalty on Digital Platforms

The effect size analysis results reveal that AI-driven personalization has a substantively strong impact on consumer trust and loyalty. The large Cohen's f^2 values (>0.35) suggest that personalization is practically significant in shaping consumer attitudes, not just statistically significant. It is important to note that perceived privacy has a medium effect on loyalty. This indicates that privacy concerns may function more as a moderating or conditioning factor rather than being the primary driver of behavioral outcomes. This supports the notion that the benefits of personalization will prevail, except in cases where the risks to privacy become apparent to users.

Table (4): Multicollinearity Diagnostics (VIF)

Independent Variable	VIF	Tolerance
Personalization Intensity	1.72	0.58
Privacy Perception	1.64	0.61
Trust	1.81	0.55

Source: Authors, PLS (2025V)

Variance Inflation Factor (VIF) values are far below the conservative threshold of 5, which indicates no multicollinearity among the explanatory variables. This finding strengthens the robustness of the regression and structural models, showing that each construct captures a different conceptual dimension and not redundant information.

Table (5): Structural Model Fit Indices (SEM)

Fit Index	Value	Recommended Threshold
χ^2 / df	2.14	< 3.00
CFI	0.94	≥ 0.90
TLI	0.92	≥ 0.90
RMSEA	0.048	≤ 0.08
SRMR	0.041	≤ 0.08

Source: Authors, PLS (2025V)

All indices exceed suggested benchmarks, demonstrating the structural equation model's outstanding overall fit. Strong explanatory coherence is indicated by high CFI and TLI scores, whereas low RMSEA and SRMR values show little residual error. These findings support the theoretical framework that links Flipkart's AI ecosystem's personalization, privacy perception, trust, and loyalty.

Table (6): Convergent and Discriminant Validity (CFA)

Construct	AVE	CR
Personalization	0.63	0.90
Privacy Perception	0.59	0.86
Trust	0.61	0.88
Loyalty	0.57	0.83

Source: Authors, PLS (2025V)

Strong convergent validity is confirmed by all constructs exceeding the suggested thresholds for Composite Reliability ($CR > 0.70$) and Average Variance Extracted ($AVE > 0.50$). This suggests that the intended latent variables are reliably captured by the measurement items. Furthermore, discriminant validity is supported by the results, guaranteeing conceptual clarity between constructs related to marketing and governance.

Table (7): Mediation Analysis – Sobel Test

Path	Z-value	Significance
Indirect Effect	4.87	$p < 0.001$
<i>(Personalization → Privacy Perception → Loyalty)</i>		

Source: Authors, PLS (2025V)

A statistically significant mediating role of privacy perception in the connection between personalization and loyalty is confirmed by the Sobel test. Although personalization directly increases loyalty, users' privacy assessments have an indirect impact as well. This research emphasizes privacy perception as a crucial psychological filter that converts AI-driven personalization into long-term customer loyalty.

Table (8): Predictive Relevance (Q^2)

Endogenous Variable	Q^2
Trust	0.31
Loyalty	0.28

Source: Authors, PLS (2025V)

Positive Q^2 values validate the structural model's predictive relevance. This suggests that the suggested governance-personalization framework has significant out-of-sample predictive power, which is a crucial requirement for theory-driven AI governance research, in addition to explaining observed relationships.

6.3. Hypotheses Testing

The main purpose of hypothesis testing in this research is to test in real life the model that connects AI-based personalization, perceived protection of data privacy, consumer trust, and loyalty to the platform Flipkart, under the laws of the Indian IT Act 2000 and SPDI Rules 2011. The hypotheses (H1–H7) that were created from the literature review will be tested through structural equation modeling (SEM), regression analysis, mediation analysis, and ANOVA for demographic differences. This paper is based on a quantitative dataset taken from 520 active users of Flipkart who represent a well-balanced sample according to gender, age groups, usage type, and frequency of purchase.

	Path	β (Standardized)	p-value	Cohen's f^2	Effect Size	Regulatory Relevance (Indian IT Act & SPDI Rules)
H1	Perceived Personalization Intensity → Consumer Trust	0.52	<0.001	0.42	Large	Trust is strengthened through explicit consent, limited data collection, and transparency, in line with IT Act 2000 & SPDI Rules 2011.
H2	Perceived Personalization Intensity → Platform Loyalty	0.48	<0.001	0.35	Large	Loyalty benefits are maximized when personalization respects purpose limitation and data retention, supporting legal compliance.
H3	Perceived Data Privacy Protection → Consumer Trust	0.41	<0.001	0.25	Medium	Compliance with consent, purpose specification, retention, and access control under SPDI Rules directly increases trust.
H4	Perceived Data Privacy Protection → Platform Loyalty	0.32	<0.01	0.25	Medium	Loyalty is reinforced when users perceive data protection is enforced according to SPDI limits, reducing perceived risk.
H5	Consumer Trust → Platform Loyalty	0.54	<0.001	0.38	Large	Trust derived from transparent, legally compliant practices encourages repeated engagement and advocacy, aligning with IT Act & SPDI requirements.
H6	Perceived Data Privacy Protection mediates	Indirect effect	<0.001	N/A	Significant mediation	Demonstrates that regulatory compliance (consent, retention,

Regulatory Compliance as a Critical Mediator Between AI Personalization and Consumer Loyalty on Digital Platforms

	Perceived Personalization Intensity → Platform Loyalty					anonymization) amplifies the impact of personalization on loyalty.
H7	Age Groups → Perceived Data Privacy Protection	F(2,517)=6.21	<0.01	N/A	Significant difference	SPDI disclosure, consent, and retention policies reduce demographic disparities in privacy perception, ensuring equitable compliance across user segments.

Source: Authors, PLS (2025V)

The conceptual framework tested seven relationships (H1–H7) through structural equation modeling (SEM), multiple linear regression, mediation analysis using Sobel test and bootstrapping, and one-way ANOVA for demographic variations. Reliability and validity of the measurement scales were established using Cronbach's alpha, composite reliability (CR), average variance extracted (AVE), and discriminant validity assessments. The dataset is in accordance with SPDI principles: responses are anonymized; participation is voluntary; data minimization applies; retention is limited for ethical compliance.

H1: Regression and SEM analyses reveal a strong positive effect ($\beta = 0.52$, $p < 0.001$, Cohen's $f^2 = 0.42$, large effect). Users who perceive high levels of personalization in recommendations, search results, and content feel more confident about Flipkart's competence and responsiveness. Regulatory relevance: Trust is strengthened under SPDI Rules and IT Act through explicit consent, limited data collection, and transparency that guarantees personalization will not compromise privacy.

H2: Results show a significant positive effect ($\beta = 0.48$, $p < 0.001$, Cohen's $f^2 = 0.35$, large effect). Personalized interactions enhance convenience and relevance to repeat purchases for long-term engagement. Regulatory relevance: Sustained loyalty requires adherence to consent and data usage disclosures so that the benefits of personalization do not undermine legal compliance.

H3: Privacy protection is an important predictor of trust ($\beta = 0.41$, $p < 0.001$; Cohen's $f^2 = 0.25$), which indicates medium effects. Users who believe that their data is being handled responsibly—through anonymization, pseudonymization, encryption as well as role-based access—are more likely to trust the system. Regulatory relevance: Compliance with SPDI Rules enhances perceptions of trust through explicit consent, purpose limitation in data collection as well as retention periods.

H4: Regression analysis suggests a moderate positive effect ($\beta = 0.32$, $p < 0.01$, Cohen's $f^2 = 0.25$, medium effect) that is consistent with the proposition that privacy assurance reduces perceived risk in repeated interactions and consequently supports loyalty. Regulatory implications are that SPDI retention limits (e.g., one month for eye-tracking data and two months for sessions) and access control measures would help sustain user engagement.

H5: SEM results reveal a significant positive relationship ($\beta = 0.54$, $p < 0.001$, Cohen's $f^2 = 0.38$, large effect), which indicates that trust plays an important relational mechanism in converting positive perceptions into behavioral loyalty. For regulatory relevance, trust from compliant practices bolsters Flipkart's credibility and ethical standing.

H6: Mediation testing through Sobel test ($Z = 4.87$, $p < 0.001$) and bootstrapped indirect effects confirms a statistically significant mediating role—indicating that personalization has a direct effect on loyalty but is stronger when users perceive data protection as robust.

Regulatory relevance lies in this mediation; it highlights how strategically significant SPDI compliance is by showing legal adherence to increase the effect of personalization on loyalty. H7: One-way ANOVA shows significant differences ($F(2, 517) = 6.21, p < 0.01$) with older and digitally less savvy users seeing higher risks regarding privacy. For regulatory relevance, SPDI disclosure requirements together with consent and retention mandates help standardize privacy perceptions across demographic segments for inclusive equitable trust-building.

Q^2 values are Trust (0.31) and Loyalty (0.28), indicating strong predictive relevance of the model.

Structural model fit is $\chi^2/df = 2.14$, CFI = 0.94, TLI = 0.92, RMSEA = 0.048, SRMR = 0.041 which demonstrates an excellent model fit.

Multicollinearity diagnostics show VIF values ranging from 1.64 to 1.81 confirming no multicollinearity.

Integrated Interpretation The testing confirms that AI-driven personalization when coupled with strong data governance and compliance with the Indian IT Act & SPDI Rules significantly enhances consumer trust and platform loyalty; perceived data privacy protection serves as both a direct influencer and a mediator highlighting the critical intersection of technological personalization behavioral outcomes regulatory compliance; age-related differences suggest demographic-sensitive transparency mechanisms are necessary to align privacy expectations with SPDI standards.

6. Implications

By empirically proving that personalization intensity increases trust and loyalty only when complemented by strong perceptions of data privacy protection, the findings tie the title of the article to visible behavioral outcomes rather than abstract regulatory discussions. In the case of Flipkart, AI-powered recommendations, personalized search ranking, and content customization become effective business tools not by themselves but as parts of a larger governance structure formed by the Indian IT Act 2000 and the SPDI Rules 2011.

The findings indicate that compliance-related practices—like explicit consent, purpose limitation, restricted data retention, anonymization of session data, and reasonable security safeguards—are not simply legal obligations but act as market-facing trust signals. These signals lower perceived risk, give legitimacy to algorithmic decision-making, and change personalization from a potentially intrusive practice into a value-adding service. In practical terms, this explains why platforms such as Flipkart—operating under heightened public scrutiny and regulatory uncertainty—cannot sustain long-term loyalty based on algorithmic sophistication alone. Instead, loyalty develops when users feel that personalization respects the limits set by Indian data protection laws and adjusts to new demands for transparency and accountability.

The mediating role of perceived data privacy protection further reinforces the article's argument by illustrating how governance quality directly conditions the commercial returns on investments in AI. Even highly accurate personalization becomes less effective if users start questioning how their data is collected, stored, or reused. On the other hand, adherence to SPDI principles enhances the positive effect of personalization on loyalty—thus demonstrating that regulatory alignment enhances rather than constrains innovation. This insight gains particular relevance in India at a time when debates about data localization spill over into discussions about cross-border data flows and hybrid datasets challenging platform governance models.

From a real-world perspective, the demographic differences in privacy perception that we observe point to the societal dimension of AI governance emphasized in the title of this article. Younger, digitally fluent users might see personalization as something normal, while older or less digitally

Regulatory Compliance as a Critical Mediator Between AI Personalization and Consumer Loyalty on Digital Platforms

experienced users depend more on visible compliance cues to build trust. This difference brings out very practically the need for platforms to implement IT Act and SPDI requirements through user-friendly consent interfaces, layered privacy notices, and clear explanations about algorithmic use—in other words bridging the gap between formal legal compliance and actual user experience.

These implications, when taken together, position AI-based personalization not as a purely technological or marketing strategy but as a regulated socio-technical system whose success in India depends on the credibility of its governance foundations. Thus, this study substantiates the article's core claim: consumer trust and loyalty are co-produced by algorithmic intelligence and regulatory compliance in Indian e-commerce. Platforms that internalize this logic will be more likely to achieve sustainable growth, mitigate regulatory risk, and maintain public legitimacy—while those that treat data governance as an afterthought will erode trust, attract legal scrutiny, and undermine the very personalization capabilities they seek to exploit.

Conclusion:

This study aims to investigate the role of AI-enabled personalization in influencing consumer trust and platform loyalty in Indian e-commerce, explicitly contextualizing these relationships within the legal provisions of the Indian IT Act 2000 and SPDI Rules 2011. Using data from 520 active users of Flipkart, it is found that perceived personalization intensity significantly drives trust and loyalty, thereby reaffirming the strategic role that AI-enabled personalization plays in creating positive consumer outcomes. However, these results indicate that such gains are not independent of governance concerns. Perceived data privacy protection is found to have a direct impact on trust and loyalty as well as acting as a mediator between personalization and loyalty; thus, personalization can be said to extract its full value only when users feel their data are managed according to regulations.

The analysis further establishes consumer trust as a pivotal relational mechanism through which technological capabilities get transformed into sustained platform engagement. Trust gets reinforced when personalization is perceived as enhancing rather than invasive, and when data practices align with legal principles such as informed consent, purpose limitation, and reasonable retention of data. The observed variation in privacy perceptions across age groups reinforces the need to factor demographic sensitivity into the evaluation of AI-driven systems as it underscores heterogeneity in user expectations within the Indian market. Collectively, these findings add to the literature by empirically demonstrating that regulatory compliance and algorithmic personalization are structurally interconnected rather than conceptually separate.

From an academic point of view, this study progresses earlier research by merging marketing theory with trust-based relational models and data governance frameworks into one explanatory model designed for a regulated e-commerce setting. It answers calls for more context-specific evidence from emerging markets while providing empirical support for governance mechanisms being not just boundary conditions but active determinants of consumer behavior in AI-mediated platforms.

Future research may further investigate these phenomena using longitudinal designs to track changes in trust and loyalty as regulatory awareness and enforcement develop. Comparative studies across platforms or jurisdictions would clarify the generalizability of the proposed framework, while deeper examination of algorithmic transparency, explainability, and ethical AI practices could improve understanding of governance dynamics beyond formal

compliance. Extending inquiry in these directions will enable future work to continue refining evidence-based models that reconcile technological innovation with consumer trust and regulatory accountability in digital commerce.

Bibliography List:

- Acquisti, A. B. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4), 736-758.**
- Anwar, M. (2021). Supporting privacy, trust, and personalization in online learning. *International Journal of Artificial Intelligence in Education*, 31(4), 769-783.
- Bag, S. S. (2022). Journey of customers in this digital era: Understanding the role of artificial intelligence technologies in user engagement and conversion. *Benchmarking: An International Journal*, 29(7), 2074-2098.
- Bilgihan, A. O. (2025). Artificial intelligence (AI) agents and the future of customer loyalty. *International Journal of Contemporary Hospitality Management*, 37(9), 3240-3262.
- Choudhary, V. &. (2023). Product recommendation and consumer search. *Journal of Management Information Systems*, 40(3), 752-777.
- Clauss, T. H. (2019). The perception of value of platform-based business models in the sharing economy: determining the drivers of user loyalty. *Review of Managerial Science*, 13(3), 605-634.
- Galvez-Cruz, D. C. (2009). An environment for protecting the privacy of e-shoppers (Doctoral dissertation, University of Glasgow).
- Jamal, K. M. (2003). Privacy in e-commerce: Development of reporting standards, disclosure, and assurance services in an unregulated market. *Journal of Accounting Research*, 41(2), 285-309.
- Jayapal, J. (2025). Unveiling the Impact of AI-Driven Personalization on Customer Loyalty in Online Shopping: The Moderating Effects of Privacy Concerns. *Journal of Promotion Management*, 1-30.
- Jayapal, J. (2025). Unveiling the Impact of AI-Driven Personalization on Customer Loyalty in Online Shopping: The Moderating Effects of Privacy Concerns. *Journal of Promotion Management*, 1-30.
- Kavitha, D. U. (2023). Super Apps: The Natural Progression in Fin-Tech. *Fintech and Cryptocurrency*, 383-412.
- Komiak, S. Y. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS quarterly*, 941-960.
- Lakasing, L. (2025). Delivering the Truth: Why NHS maternity care is broken and how we can fix it together. Right Book Press.
- Lamarre, E. S. (2023). Rewired: the McKinsey Guide to Outcompeting in the Age of Digital and AI. John Wiley & Sons.
- Lee, J. L. (2015). Antecedents of cognitive trust and affective distrust and their mediating roles in building customer loyalty. *Information Systems Frontiers*, 17(1), 159-175.
- Lund, S. M. (2021). What's next for consumers, workers, and companies in the post-COVID-19 recovery. *McKinsey & Company*, 2(11).
- Mohammadi, V. R. (2019). Trust-based recommendation systems in Internet of Things: a systematic literature review. *Human-centric Computing and Information Sciences*, 9(1), 21.
- Morgan, G. &. (2018). Regulatory compliance. In *Regulation and organizations* (pp. 166-190). Routledge.
- Morgan, R. M. (1994). The commitment-trust theory of relationship marketing. *Journal of marketing*, 58(3), 20-38.
- Prasanna, R. J. (2025, November). How Intellectual Property Boosted the Valuation of Indian Startups—A Deep Dive Into Byju's and Ola: Case Study. In *2025 9th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-6). IEEE.
- Saxena, U. R. (2023). Provisioning trust-oriented role-based access control for maintaining data integrity in cloud. *International Journal of System Assurance Engineering and Management*, 14(6), 2559-2578.
- Thaichon, P. L. (2020). Online relationship marketing: evolution and theoretical insights into online relationship marketing. *Marketing Intelligence & Planning*, 38(6), 676-698.
- Theodorakopoulos, L. &. (2024). Leveraging big data analytics for understanding consumer behavior in digital marketing: A systematic review. *Human Behavior and Emerging Technologies*, 2024(1), 3641502.