Journal of
Theoretical and Applied Electronic Commerce Research

MDPI

Article

The Impact of Integrity-Related Factors on Consumer Shopping Intention–An Interactive Marketing Approach Based on Digital Integrity Model

Nicoleta-Valentina Florea [1], Gabriel Croitoru [1,*] and Aurelia-Aurora Diaconeasa [2]

[1] Department of Management and Marketing, Faculty of Economic Sciences, Valahia University of Târgoviște, 130004 Targoviste, Romania; nicoleta.florea@valahia.ro
[2] Faculty of Economics, Valahia University of Târgoviște, 130004 Targoviste, Romania; diaconeasa.aurora@valahia.ro
* Correspondence: gabriel.croitoru@valahia.ro

Abstract

The purpose of this study is to examine the impact of integrity-related considerations, such as ethics, privacy, protection, security, and trust, on online consumer shopping intention within the interactive marketing environment. To achieve this, the research uses partial least squares structural equation modelling (PLS-SEM), analysing data from a sample of 260 respondents collected through an online survey. The findings reveal that protection is the most influential factor driving consumer buying intentions, followed by trust, ethics and security. Privacy, while significant, has a more moderate influence on consumer behaviour compared to other factors. The study makes a key theoretical contribution by advancing the understanding of how these constructs interact to shape consumer behaviour in the digital marketplace, particularly highlighting the importance of data protection and ethical practices. Practically, the research offers actionable recommendations for e-commerce businesses, based on building a digital integrity model, suggesting the focus on enhancing data security and ethical transparency to build consumer trust. Furthermore, the findings highlight the need for policymakers to strengthen data privacy regulations and harmonise international security standards in e-commerce. Future research should consider longitudinal studies and explore these dynamics in different regulatory environments.

Keywords: e-commerce; integrity-related factors; consumer shopping intention; interactive marketing environment; digital integrity model; e-platforms performance

check for updates

Academic Editors: Ting Chi, Chenglu Wang, Hongfei Liu, Morgan Yang, Qing Ye and Yunjia Chi

Received: 17 July 2025
Revised: 8 September 2025
Accepted: 9 September 2025
Published: 1 October 2025

Citation: Florea, N.-V.; Croitoru, G.; Diaconeasa, A.-A. The Impact of Integrity-Related Factors on Consumer Shopping Intention–An Interactive Marketing Approach Based on Digital Integrity Model. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 262. https://doi.org/10.3390/jtaer20040262

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Recent research highlights the critical role of privacy and security in shaping consumer trust and purchasing intentions in e-commerce, security and trust play an important role in obtaining user satisfaction because e-commerce has achieved rapid growth in the global economy [1]. Previous studies have examined these factors individually, but a comprehensive and integrated perspective remains underexplored.

Recent studies demonstrate the complex interplay between consumer perceptions, privacy concerns, and trust in the digital marketplace, showing that privacy risks significantly shape trust formation and purchase intentions in online settings [2–4]. Studies indicate that factors such as perceived security, privacy, and reputation significantly influence consumer trust and willingness to purchase online [2,3], being very important factors in social media platforms and interactive marketing [4–9].

The power–responsibility equilibrium theory suggests that deficiencies in corporate privacy responsibility and regulatory protection can lead to decreased consumer privacy empowerment and increased concerns [10,11]. Cross-cultural studies reveal variations in privacy perceptions and their impact on trust and behavioural intentions [12]. Researchers emphasise the need for a comprehensive approach to address privacy issues, considering the perspectives of behavioural economics and the broader implications for sustainable economic development [13,14]. In the context of sustainable products, trust emerges as a critical factor influencing online purchase intentions, with perceived risk, security, and privacy as key determinants [15].

In the rapidly evolving digital landscape, understanding the factors that influence consumers' purchasing intentions in e-commerce is important. Privacy, ethics, data protection, security, and trust are essential elements that shape these intentions. This analysis synthesises information from various studies to explore how these factors influence consumer behaviour in online environments, providing a comprehensive overview of their roles in improving the online shopping experience and promoting consumer loyalty.

In the digital age, data privacy has become an important factor in influencing online shopping behaviour. Consumers, increasingly aware of the risks associated with exposing personal data, express their concerns through increased caution in online transactions. This caution is justified, as privacy issues directly affect consumer trust and, consequently, purchasing intentions. Recent studies [16] indicate that perception of privacy control can alleviate these concerns, but this effect depends on individual factors such as the consumer's previous experience with online privacy and their level of risk aversion. Thus, in response to these concerns, the implementation of robust data protection laws, as seen in Indonesia and India, plays an essential role. These legislative frameworks not only ensure data security and transparency, but also enhance consumer trust by reducing perceived risks [17]. Beyond legality, ethics play a vital role in e-commerce. The ethical practices of merchants are essential to build a climate of trust and consumer satisfaction. Ethical perceptions not only influence purchasing intentions but are mediated by the trust consumers place in the platform. Solid ethical behaviour can lead to increased customer loyalty, underscoring the importance of integrity in online commerce [18]. In the same vein, data security becomes a fundamental element that influences purchasing decisions. Consumers tend to prioritise platforms that provide guarantees of data protection, which directly affects their intent to make repeat transactions. For example, on platforms such as Shopee Indonesia, perceived security has been highlighted as a major factor influencing repurchase behaviour [19]. Ultimately, trust lies at the foundation of the entire e-commerce ecosystem, a central element that profoundly influences purchasing decisions. Trust acts as a bond between security, privacy, and buying intentions, demonstrating its important relevance in the digital marketplace [20,21]. It transcends socioeconomic differences and levels of digital participation, highlighting its role in reducing perceived risks and strengthening consumer trust in online interactions [22]. The interaction between privacy, ethics, security, and trust forms a complex web that shapes consumers' purchasing intentions. Companies must adapt to these complexities and overcome regulatory challenges to create a safe and reliable online environment. Only then will they effectively meet the diverse needs of modern consumers, ensuring the sustainability of their businesses in the digital world.

This study aims to formulate and explore supportive research questions that are deeply interconnected with the proposed objectives, namely: How does the perception of data privacy influence your intention to make online purchases? This question focuses on assessing the impact of consumer perceptions regarding the level of personal data protection on purchasing decisions, considering that, in the context of accelerated digitalisation, the degree of data protection becomes an essential factor in establishing consumer trust.

Additionally, it analyses the extent to which the ethics of e-commerce companies affect consumer buying behaviour, exploring the impact of transparency, fairness, and adherence to moral standards on consumer choices. It is also essential to determine the impact of data protection on the level of consumer trust in e-commerce platforms by evaluating the contribution of protective measures to building and maintaining a climate of trust. Another important dimension of the research focuses on the role of security in e-commerce platforms in consumers' decisions to shop online, measuring the effectiveness of security in preventing fraud and protecting transactions in relation to customer loyalty. Finally, it investigates the extent to which consumer trust in these platforms influences purchase intention, highlighting the importance of trust in recommendations and repeat purchases. Through these questions, the research aims to clarify the mechanisms by which factors such as privacy, ethics, data protection, security, and trust shape consumer behaviours in online environments and impact their purchasing decisions.

Wang's study is particularly relevant in the context of interactive marketing, which investigates the interactions between marketing systems and society, analysing the impact of marketing practices on the general well-being of consumers and the economy [5]. In the digital age, where e-commerce plays an increasingly important role in daily life, aspects such as data privacy, ethics, data protection, security, and trust have become essential elements in shaping commercial relationships between consumers and companies [23]. From the perspective of interactive marketing, this study provides a detailed understanding of how these variables not only influence individual purchasing behaviour but also contribute to the balance between economic efficiency and social well-being. By investigating factors that affect consumer trust in e-commerce platforms and the intention to make online purchases, the study contributes to the debates surrounding the social and economic impact of digital commerce. Another essential aspect of the importance of this study for interactive marketing is its contribution to a sustainable digital economy. Consumers are no longer just passive buyers, but active participants who express their expectations regarding data protection and transaction security. E-commerce firms must respond to these demands to create a trustworthy environment where consumer rights are respected and commercial relationships are fair and transparent. By incorporating these elements into their strategies, companies not only protect their reputation but also contribute to the development of a more responsible and ethical economic environment. The study adds value to the interactive marketing literature by highlighting critical relationships between consumer behaviour and systemic changes in the digital economy. In a world where e-commerce is largely dependent on the trust and security perceived by consumers, understanding these dynamics is vital to designing policies and marketing strategies that ensure the long-term sustainability of the digital economy and support responsible innovation.

Thus, this research not only provides practical insight for companies but also has significant implications for public policies, contributing to the development of regulations that ensure fairness and security in the digital environment, benefiting consumers and the global market.

This study introduces a novel digital integrity model that differs from existing frameworks by integrating privacy, ethics, protection, security, and trust into a unified construct and incorporating empirically derived relative weights, estimated through the PLS algorithm, to reflect the varying importance of each factor in context. Unlike prior models that analyse these elements in isolation, our approach emphasises their synergistic effects on consumer online shopping intention, thereby providing both a theoretical advancement and a practical decision-making tool for e-commerce platforms.

The structure of the articles is as follows. In the first section, the literature review in the field, the research hypotheses are developed, and the conceptual model is built according

to the studies. The second section describes the sample and the demographic analysis of the sample. The third section presents the analysis, the results, the discussion, and the theoretical and practical implications. Limitations are presented and future research directions are presented.

2. Literature Review and Supporting Theories

Though e-commerce is increasing in the world in terms of usability, in the minds of customers, there are some factors that can affect the e-commerce performance [24].

Studies show that perceived privacy, security, and reputation significantly influence trust and willingness to buy online [2,25]. Consumers are particularly concerned about data collection, storage, and sharing practices [26]. Trusted websites with clear privacy policies and secure systems tend to decrease privacy concerns and encourage online shopping [26,27]. Trust, perceived risk, and e-WOM are key factors that affect e-commerce purchasing decisions, with perceived risk moderating the relationship between trust and buying intentions [22,28]. Ethical performance of e-commerce websites improves customer trust, commitment, and loyalty [25]. Understanding consumer perceptions of privacy is important to understanding online behaviour and promoting e-commerce adoption [29].

Although protection, security, and ethics may appear conceptually close, prior literature highlights their distinct theoretical roles in digital commerce. Protection refers primarily to the formal mechanisms that safeguard consumers, such as legal frameworks, data protection policies, and institutional regulations designed to ensure responsible handling of personal and transactional data. In contrast, security captures the technical and procedural measures adopted by platforms, including encryption, authentication, and fraud-prevention systems, which directly mitigate transaction-related risks. Ethics, however, extends beyond compliance and technical safeguards to encompass the normative dimension of organizational conduct, including fairness, transparency, and avoidance of manipulative practices in digital interactions.

Empirical evidence supports these distinctions. Regulatory protection mechanisms have been shown to reinforce consumer trust in cross-border digital transactions [30]. Security features such as multifactor authentication directly reduce risk perceptions and improve adoption of online services [31]. Ethical practices, such as transparency and integrity in data usage, play a critical role in sustaining long-term trust [32]. Therefore, despite their conceptual proximity, the three constructs reflect complementary but distinct facets of consumer experience in e-commerce and are treated as separate latent variables in the digital integrity model.

The digital integrity model proposed in this study integrates five key constructs—data privacy, ethics, data protection, security, and trust—as determinants of consumer shopping intention in e-commerce. These constructs were selected because they consistently emerge in prior literature as central to consumer perceptions of fairness, safety, and credibility in digital environments, unlike other factors such as convenience or usability, which are more operational in nature.

By distinguishing between privacy (perceptions of individual control) and data protection (formal safeguards and compliance mechanisms), the model avoids conceptual overlap and reflects both consumer-centric and institutional perspectives. Terminology is used consistently across hypotheses and analyses: the outcome construct is referred to throughout as consumer shopping intention in e-commerce.

Based on this conceptual foundation, the subsections that follow (2.1–2.5) review the literature supporting each construct and present the development of Hypotheses H1–H5.

2.1. Privacy

Recent studies highlight the growing importance of data privacy in e-commerce, emphasising that consumers' willingness to engage with online platforms is strongly influenced by transparent data-handling practices [33,34]. Implementing stricter privacy regulations such as GDPR and CCPA has reinforced perceived control and mitigated privacy concerns in digital contexts [35].

The use must offer customers when visiting a website comfort and ease of use based on previous experiences [36], and the privacy of the data [37].

Privacy is about offering guarantees [38], confidentiality, and safety of private information according to privacy standards [39]. It offers the customer the assurance of not being able to lose personal information in transactions made through the system [40]. Privacy in e-commerce is a sensitive issue because it involves the use of customers' personal data. According to consumer rights and privacy policies, personal information must be protected [41]. Privacy matters can lead to negative experiences and make customers more cautious about sharing personal information [16]. To overcome these issues, companies may use intrusion detection algorithms [42]. Customer trust is recognised as one of the most important aspects of using e-commerce [43]. The lack of trust is an important barrier to online shopping intentions [44]. Studies have shown that the privacy of data has an influence on the intention to buy online. Research in 557 respondents from China indicated this influence [45]. According to these, we may develop the following hypothesis as

H1: *There is a positive impact of customer transaction privacy on consumer shopping intention in interactive marketing environment.*

2.2. Ethics

Recent research highlights the growing importance of ethical business conduct in digital commerce for customer retention and brand trust. Studies show that sustainable digital marketing practices, including transparency and stakeholder engagement, positively impact brand reputation and consumer engagement [46].

Ethics is important for both parties involved in e-commerce, the customer and the company. The freedom to not violate the specifications written on the website, to have transparency conditions, not manipulate based on prices, not discriminate and not offer equal treatment according to the norms are important in online commerce [47]. In addition, ethics is an important norm in digital marketing as a strategy to improve customer relationships and e-commerce usability [48].

To survive in this challenging interactive marketing environment, companies may use dark patterns to manipulate customer decision-making [49]. To increase the intention to buy online, companies are using processes based on prudence, industriousness, genuineness, sacrifice spirit and self-command, in order to increase performance [50].

Online purchases increased, especially during the coronavirus pandemic, and in this period, ethical and legal issues appeared, growing in intensity [51]. To protect data, normative laws and big data regulations were developed. Because e-commerce is an insecure place to protect customer data from being stolen or used by other companies without the customer's consent. A study demonstrated that laws cannot keep pace with technological developments and provide effective protection [52]. Another study using PLS-SEM conducted on 1032 users in Colombia demonstrated that ethics influences trust and customer experience when using e-platforms [53].

Ethical concerns are important and are evident in consumer reviews of e-platforms. Ethics also depends on the information quality used on the website, so the accuracy and authenticity of the information on products must be true [54]. However, many customers

are sceptical about using e-commerce due to perceived high risks and uncertainty [28,55,56]. Therefore, the second research hypothesis was developed as

H2: *There is a positive impact of consumer ethics on e-commerce shopping intention in interactive marketing environment.*

2.3. Data Protection

Consumer protection mechanisms play an important role in enhancing trust and reducing purchase hesitation in e-commerce, particularly in high-risk contexts. Conceptually, *protection* refers to institutional and regulatory safeguards that govern the responsible handling of consumer data, such as legal frameworks, privacy regulations, compliance policies, and formal organisational procedures [57–59]. These mechanisms establish a structural basis for consumer confidence, signalling that transactions are conducted under enforceable standards of security and fairness.

At the same time, consumers often assess protection not only through abstract regulations, but also through concrete cues available on digital platforms. Elements such as customer reviews, FAQ sections, or clearly stated service policies act as perceived signals that protective mechanisms are active and transparent. Although such signals may also be associated with information quality or transparency, previous research shows that users interpret them as indicators that institutional protections are in place and effective [60–62]. Therefore, in this study, these consumer-facing items are retained within the protection block to reflect how users operationalise their sense of being protected in online environments.

Empirical findings confirm the importance of protection mechanisms. Regulatory safeguards reinforce trust in cross-border digital trade [63], while security policies such as encryption and password management significantly reduce risk perceptions [64]. Surveys indicate that more than half of respondents consider formal protection measures to be effective in ensuring safe transactions [65]. Thus, another research hypothesis,

H3: *There is a positive impact of consumer data protection on e-commerce shopping intention in an interactive marketing environment.*

2.4. Security

Recent studies highlight the critical role of trust and security in driving the adoption of digital technologies across various domains. Enhanced security features, transparent privacy policies, and user empowerment consistently improve consumers' trust and behavioural intentions toward digital services [66]. Trust significantly influences perceived usefulness and adoption of digital payments [67], while also mediating the relationship between perceived risks and satisfaction in cross-border e-commerce [68].

Security is about ensuring secure guarded information from consumers and company databases [69] and protecting from unauthorised access. Studies indicated that security is the most important ethical factor in e-commerce [70]. Security breaches are appearing every day, giving e-consumers real worries, so services provided by online platforms must reduce risks. Companies must be prepared with measures and solutions to protect customers from internet malpractices [31], fraud, attacks, and errors [71]. Many studies analysed issues about assurance, warranties and website and service quality [72], lack of trust and security due to the growth of e-commerce [60]. The transactions between consumers and companies are based on the use of websites [73], and barriers are present at every step, such as information security and threats [74]. This important issue will slow the use of the internet and e-commerce growth, leading to a loss of confidence [75].

Most e-consumers are very concerned about the lack of security of their personal information because the companies may send them unsolicited materials, send their personal information to third parties, and commit fraud (credit card information) [76].

Based on these ideas, another hypothesis was developed as

H4: *There is a positive impact of consumers' security on e-commerce shopping intention in an interactive marketing environment.*

2.5. Trust

Trust remains a critical factor in online shopping in various markets, mediating the effects of risk perception and security [57,58]. It plays a pivotal role in shaping consumer satisfaction and purchase intentions [68]. Trust is influenced by factors such as reputation, transaction safety, and economic viability [59]. Platform governance mechanisms, including normative and relational approaches, can improve seller trust in cross-border e-commerce [77].

When e-commerce appeared, companies and customers aimed to have a trustworthy and fair environment for e-shopping [78]. Thus, trust is another important factor for an online interactive marketing environment [79]. Trust is an anticipation of a company's promise not to take advantage of the customer's weakness, being a factor in the success of e-platforms [78]. There are a few attributes to increase consumer trust of consumers [80] from the company—telephone number, email address, privacy policy, company address, merchant trust, from third party (to secure transactions, to secure data), from consumer (feedback, recommendation) and from employees (names, photo).

Trust in an interactive online environment:

- is a vital factor in ensuring performance for both parties and lack of trust will affect this performance in the online interactive environment [81].
- creates a social atmosphere where organisations can work with customers and is seen as a powerful marketing tool based on a trust relationship [82].
- reduces social complexity [83] and therefore an ecommerce application should integrate trust, in both environments: physical and virtual [84].

Some important models were developed by experts in the field in order to build trust in e-commerce [85–87].

Customers want to trust in the company's actions and not sell, offer data about them, or protect them from breaches [88]. They also want a trustworthy environment due to the lack of presence (thus companies implemented online shopping assistants), but enjoy convenience, easy access to information, variety of products or services, and discounts [89]. Trust influences the intention to buy online and amplifies the importance of minimizing the risks in e-commerce [22]. Lack of trust is a barrier to intention to use e-commerce [90], trustworthiness being among the most important factors that make the difference between buyers and non-buyers and a critical factor for e-commerce performance [91] and for improvement of social and economic interactions [92].

Trust is also on reduced perceived risk [93], website quality and reputation [94], integrity [73], and service quality [95,96]. A study conducted on 386 Indian students demonstrated that trust in using a website is very important using PLS-SEM [97]. Other studies in the field demonstrated that trust influences intention to buy online using websites [98,99], using PLS-SEM [100], security [101,102], and ethics with a direct influence on the behavior [103]. Thus, the final hypothesis was developed as

H5: *There is a positive impact of consumer trust on e-commerce shopping intention in interactive marketing environment.*

The novelty of the digital integrity model lies in its integration of key constructs (privacy, ethics, data protection, security, and trust) within a unified framework, and in highlighting their empirically determined relative importance, as estimated by PLS. Previous research has shown that the relative importance of these factors varies in contexts—for example, security concerns can dominate financial transactions [104], while privacy or ethical considerations may be more prominent in social commerce settings [105]. By incorporating the principle of contextual varying importance, our model avoids assuming a static hierarchy of predictors and instead allows empirical estimation of the relative contribution of each construct. This ensures greater adaptability and comparability across digital environments.

3. Research Methodology

3.1. Data Collection and Sampling

Data collection was carried out through an online questionnaire using the Google Forms platform, targeting a sample of 260 respondents. The sampling criteria required participants to be active users of e-commerce platforms in the last 12 months, with at least one completed online purchase. To ensure diversity, the sample included respondents of multiple age categories (18–24, 25–34, 35–44, 45–54, 55+) and a range of income levels, from below the national average to above-average earnings. This approach was designed to capture a broad spectrum of consumer behaviours and perceptions in different socioeconomic groups. These respondents, Romanian Internet users, were selected based on diversity criteria such as age, gender, education, and frequency of Internet use. Romania constitutes a pertinent research context by combining the characteristics of a rapidly expanding digital economy with those of a member state of the European Union subject to strict regulatory frameworks. Acceleration of digital adoption, increased digital literacy, and rigorous enforcement of GDPR regulations significantly influence consumer expectations about privacy, security, and trust. This dual positioning enables Romania to be illustrative both of emerging digital markets and of highly regulated European environments, offering insights that may prove valuable for understanding similar dynamics in other countries undergoing concurrent processes of market development and regulatory alignment. The selection process was based on the principle of convenience, facilitating access to respondents through the online environment, with the aim of exploring consumer perceptions regarding the factors studied. Participation was voluntary and respondents were informed of the anonymity of the data and its use solely for academic analysis, with the option to withdraw from the study at any time. To ensure sample adequacy, we applied both the "10× rule" commonly recommended in PLS-SEM and an a priori power analysis. According to the 10× rule [106], the minimum required sample size is ten times the largest number of arrows pointing to a construct (5 for shopping intention, requiring 50 cases) or ten times the largest number of indicators in a construct (4 items, requiring 40 cases). Both criteria suggest a minimum of 40–50 respondents. Furthermore, an a priori power analysis using G*Power 3.1.9.7. [107] for a model with five predictors, medium effect size ($f^2 = 0.15$), $\alpha = 0.05$ and statistical power of 0.80 indicated a minimum of 92 respondents. Our sample of 260, therefore, exceeds all recommended thresholds, ensuring sufficient power and robustness of the results.

3.2. Survey Instrument Development

The questionnaire was designed to systematically analyse respondents' perceptions of privacy, ethics, data protection, security, trust, and online purchasing intention. Structured into two sections, the first segment addressed demographic data, requesting essential information such as age, sex, education level, monthly income, and frequency of internet

use, to provide an appropriate social and economic context. The second segment, using a Likert scale (1—total disagree and 5—total agree), assessed the degree of agreement among respondents with various relevant statements, allowing for a detailed analysis of attitudes towards the targeted themes. This rigorous methodology ensured an objective evaluation of critical variables in online consumer behaviour. To comprehensively assess the user experience in the digital environment, each variable was analysed through a set of structured questions focusing on essential dimensions. Privacy, ethics and information security were key priorities, addressing aspects such as the reuse of personal data, controlled access, and quality of communication, thus providing an overview of the security of sensitive information. Additionally, data protection was investigated by evaluating security certification and return policies, while consumer behaviour was influenced by trust in online payments and social interactions. This detailed analysis enabled the identification of key factors that determine purchasing intent and the frequency of interactions with e-commerce platforms.

The constructs selected for this study—privacy, ethics, protection, security and trust—were identified based on their consistent theoretical and empirical relevance in explaining consumer behaviour in e-commerce, as detailed in Sections 2.1–2.5. Each has been shown to directly influence online shopping intention and loyalty, making them essential components of the proposed digital integrity model. Privacy and protection address consumers' concerns about the handling of personal data and safeguards against misuse; ethics reflects perceptions of fairness, transparency and responsible corporate conduct; security captures technical and procedural measures that reduce perceived risk; and trust represents the overarching belief in the reliability and integrity of the e-commerce platform.

The cultural context of the research is equally important. Romania, as an emerging digital economy within the European Union, offers a distinctive environment characterised by rapid e-commerce growth, evolving consumer expectations, and increasing awareness of privacy and security issues due to both local market developments and EU regulatory frameworks such as GDPR. Cultural norms influence how consumers perceive trust, evaluate ethical practices, and respond to security guarantees, which may moderate the constructed concepts' relationships between the studied and the purchase intention. Understanding these dynamics not only strengthens the applicability of the findings to the Romanian market, but also provides relevant information to other regions with similar socioeconomic and regulatory conditions.

Further details on the adaptation protocol, pilot testing, and the construct validation process, including the selection of items and exclusion criteria, are provided in Section 3.5 (Measurement Tools) and Appendix A.

3.3. Respondent's Summary

The demographic profile of the respondents is particularly relevant in the analysis of this study, considering that demographic variables shape perceptions of privacy, ethics, data protection, security, and trust, essential factors that influence online purchasing intentions. Demographic classification by age is justified by the significant impact it has on online behaviour. Young people, especially those of the Millennial and Gen Z generations, are much more open to e-commerce but are also more cautious about privacy and data security issues due to their familiarity with technology. On the contrary, older people tend to be hesitant about these transactions, valuing trust and security. A deep understanding of these differentiated perceptions based on age is essential to formulate personalised recommendations that can improve user experience on e-commerce platforms. Gender, level of education, monthly income, and frequency of Internet use prove to be fundamental variables in shaping consumer purchasing behaviour on e-commerce plat-

forms. Studies show that women, aware of the risks associated with online security, are more inclined to prioritise the protection of personal data, while men exhibit a stronger preference for efficiency and the overall transaction experience. Classifying respondents by education level reveals a significant correlation between higher education and a deeper understanding of individual rights in the digital environment; thus, educated people tend to be more reserved when exposing personal information. Furthermore, monthly income influences not only purchasing behaviour but also perceptions of transaction safety, with higher income consumers having stricter demands regarding security, while those with lower incomes exhibit increased caution. Finally, the frequency of Internet use determines the variability of perceptions related to security and privacy, and frequent users develop a greater awareness of risks. Thus, analysing these factors provides a solid foundation for e-commerce companies to adapt their marketing strategies to the diverse needs of consumers.

Providing demographic details is fundamental for understanding the variability of respondents' perceptions regarding the investigated factors. By diversifying the sample based on these characteristics, a comparative analysis is facilitated between different demographic groups, highlighting significant differences in online consumer attitudes and behaviours. This approach allows for the identification of more vulnerable segments or those that require specific strategies related to privacy, security, and trust in e-commerce, offering companies a solid foundation for adapting their marketing strategies (Table 1).

Table 1. Demographic characteristics of the respondents.

Demographic Characteristics		n = 260	Percent
Age	18–24 years old	66	25.4
	25–34 years old	78	30.0
	35–44 years old	52	20.0
	45–54 years old	39	15.0
	55–64 years old	21	8.1
	Over 65 years	4	1.5
	Total	260	100.0
Gender	Male	98	37.7
	Female	162	62.3
	Total	260	100.0
Level of education	Bachelor's studies	103	39.6
	Master's studies	39	15.0
	Doctoral studies	15	5.80
	Middle school studies	11	4.20
	High school studies	66	25.4
	Vocational studies	26	10.0
	Total	260	100.0
Monthly income	1000–2000 EUR	103	39.6
	2000–3000 EUR	39	15.0
	Over 3000 EUR	15	5.8
	Under 1000 EUR	103	39.6
	Total	260	100.0

Table 1. *Cont.*

Demographic Characteristics		n = 260	Percent
Internet usage frequency	A few times a week	52	20.0
	Less often	11	4.2
	Once a week	14	5.4
	Daily	183	70.4
	Total	260	100.0

Source: Authors' own work.

In general, the demographic profile of the respondents reflects a predominantly young, educated and active online population, essential characteristics to understand the criteria that govern consumer behaviour in the digital age. These individuals, distinguished by their openness to technology and increased familiarity with e-commerce platforms, are significantly influenced by aspects such as the privacy of personal information, the ethics of business practices, the protection of sensitive data, the security of online transactions, and, not least, the degree of trust they feel towards the brands they are interested in. The significant presence of women in the sample proves to be an important factor, providing valuable insights into the specifics of purchasing behaviour, as well as the concerns related to information security and privacy, areas that are becoming increasingly important in contexts of online interaction. Furthermore, the high level of education among the respondents suggests a deep awareness of ethical issues and data protection, aspects that can directly influence not only trust in online shopping platforms but also the concrete intention to make purchases. The distribution of income within the sample reveals that the price and perceived value of the products are determining factors in the decision-making process for most of the respondents, thus highlighting the importance of transparency and fairness in commercial offers. Additionally, the high frequency of Internet use underscores the relevance of the sample for studying the phenomenon of e-commerce and the variables that contribute to its development. This detailed analysis of demographic characteristics not only illustrates the nuances of consumer behaviour, but also emphasises the necessity for marketing strategies and security measures adopted by e-commerce companies to be tailored to the needs and expectations of various consumer segments. In conclusion, a deep understanding of the demographic profile of users is essential to foster trust and significantly improve the online shopping experience, thus promoting a closer and more satisfying relationship between consumers and companies.

3.4. Common Method and Non-Response Bias

To minimise the risk of common method bias (CMB), respondents were assured of the anonymity of their responses and the confidentiality of the information provided. The questionnaire was carefully designed using neutral wording and a clear structure to reduce social desirability bias and response pressure.

To further examine the potential influence of CMB, we employed Harman's single-factor test [108]. All measurement items were entered into an exploratory factor analysis using principal component extraction without rotation. The results revealed that the first factor accounted for only 41.88% of the total variance (Table 2). Since this value is below the recommended threshold of 50%, we conclude that CMB is unlikely to pose a serious threat to the validity of our findings. These results, together with the procedural remedies applied during survey design (e.g., anonymity, neutral wording, counterbalancing of item order), provide support that common method variance is not a significant concern in this study.

Table 2. Harman's single-factor test results.

Component	Eigenvalue	% of Variance	Cumulative %
First Factor	10.051	41.88%	41.88%

To further assess potential non-response bias, we compared early respondents (first 30% of responses) with late respondents (last 30%), based on the assumption that late respondents serve as proxies for non-respondents [109–111]. Independent sample *t*-tests conducted across all constructs (privacy, ethics, protection, security, trust, and intention) showed no statistically significant differences between the two groups (all $p > 0.05$; Table 3). These findings provide strong evidence that non-response bias is not a concern in our study.

Table 3. Test for non-response bias (early vs. late respondents).

Construct	Mean (Early)	Mean (Late)	*t*-Value	*p*-Value
Privacy (P)	4.46	4.35	1.22	0.22
Ethics (E)	4.03	3.89	1.46	0.15
Protection (Pr)	4.19	4.13	0.89	0.38
Security (S)	4.36	4.24	1.26	0.21
Trust (T)	4.41	4.35	0.92	0.36
Intention (IC)	4.25	4.19	0.84	0.40

Note: Independent sample *t*-tests between early (first 30%) and late (last 30%) respondents. No significant differences found (all $p > 0.05$).

3.5. Measurement Tools

Our constructions are grounded in validated models from the specialised literature, ensuring solid theoretical foundations and rigorous operationalisation. This methodological approach not only supports the validity of our hypotheses but also enables a detailed analysis of variable interactions. By integrating these models into our research, we ensure a rigorous structure that supports coherent data interpretation and advances knowledge in our field. Therefore, our objective is to contribute significantly to the specialised literature by highlighting the nuances and complexities of identified relationships.

The exact survey wording, the provenance of the items, and the alignment are provided in Appendix A (Table A3).

In this study, protection is conceptually defined as institutional and regulatory safeguards that ensure responsible handling of consumer data, such as legal frameworks, compliance policies, and formal security standards. At the operational level, however, protection also includes consumer-facing cues such as customer reviews or FAQ sections. Although these items could alternatively be classified under transparency or information quality, previous literature indicates that users interpret them as signals of the presence and effectiveness of protective mechanisms. We therefore retained them within the protection block to capture the way consumers perceive and evaluate safeguards in online environments. This operationalisation is consistent with earlier studies and is further discussed in the limitations section as an area for refinement in future research.

To ensure the cultural and linguistic validity of the measurement instruments, we followed a rigorous adaptation protocol aligned with best practices [112,113]. English elements were translated into Romanian through a two-step back-translation process involving two independent bilingual translators. A panel of three domain experts then reviewed the translations for conceptual equivalence and cultural relevance. Subsequently, we conducted cognitive interviews with five representative respondents to assess item

clarity and contextual fit, followed by a pilot test with 30 participants. Feedback from these stages informed minor language adjustments, preserving both the psychometric integrity of the original scales and their suitability for the Romanian context. During the pilot testing stage, inter-item and item-total correlations were examined to assess the internal consistency of the measurement scales. All items retained met the recommended thresholds (inter-item > 0.30; item-total > 0.40), confirming satisfactory homogeneity. Additionally, preliminary qualitative work was carried out before the launch of the survey, including two focus groups (n = six participants each) and three in-depth interviews with frequent online shoppers. These sessions provided valuable feedback on the clarity of the language, cultural nuances, and contextual relevance, which informed minor adjustments to the final survey instrument.

To ensure the validity of the constructs, an exploratory factor analysis (EFA) was conducted on the pilot data. Based on the predefined criteria (factor loadings ≥ 0.60 and no cross-loadings > 0.40), several items were excluded, as shown in Appendix A (full wording of excluded items is provided for transparency). The removal of these elements aimed at improving internal consistency and convergent validity of the constructs retained in the final model.

The results of the sample adequacy tests confirmed the suitability of applying EFA. The KMO values for each construct exceeded the recommended threshold of 0.70, indicating satisfactory sampling adequacy, while the Bartlett test was statistically significant for all sets of items ($p < 0.001$), confirming sufficient correlations (Table A1). For each construct, a single dominant factor was retained, explaining between 59% and 71% of the variance, while at the global level, the five retained factors accounted for 77.03% of the total variance. The extraction method employed was principal component analysis (PCA) and the rotation method was Varimax with Kaiser normalisation.

To assess common method bias (CMB), we used both Harman's single-factor test and the full collinearity approach [114]. The full-collinearity test evaluates variance inflation factors (VIFs) for all latent constructs; values below 3.3 are typically considered evidence of no CMB. In our model, most full-collinearity VIFs were below this threshold, while a few items slightly exceeded it (maximum = 4.22). As all values remained well below the more conservative threshold of 5.0 [115], we conclude that CMB is unlikely to pose a serious threat to the validity of the results.

Standardised factor loadings for the retained items are presented in Table A2, showing that each indicator loaded strongly on its respective theoretical construct, with no notable cross-loadings. This confirms the robustness of the factor structure and supports the retention of the five factors corresponding to the theoretical constructs: privacy, ethics, protection, security, and trust.

Although some of the original scales employed in this study were developed in the late twentieth century [16,116,117], they remain widely cited and validated across diverse contexts, including recent e-commerce research [106,118,119]. Their enduring theoretical robustness ensures comparability with previous studies and facilitates the building of cumulative knowledge.

To address potential limitations related to outdated item wording or scope, we adapt the constructs to reflect contemporary digital environments. This process involved an expert evaluation of the relevance of the item, the incorporation of updated terminology (e.g., replacing "computer" with "online platform"), and the inclusion of contextual references to current privacy regulations such as GDPR and CCPA. The adaptation ensured that the measurement tools captured not only the foundational dimensions of each construct but also their modern manifestations in the interactive marketing and e-commerce landscape of today.

3.6. Model-Based Explanations

Building on validated models from the literature (Table 4) and extending them, a new model called the "digital integrity model" is proposed, unifying all these variables under a single concept. The proposed model suggests that digital integrity, comprising confidentiality, ethics, protection, security, and trust, significantly affects online purchase intention. In this context, we integrated validated dimensions and measurement tools, adapting them to the new challenges and requirements of the contemporary e-commerce environment. This model (Figure 1) offers an integrated and clear perspective on the factors that influence the intention to buy online, based on trust, security, and digital ethics, which are essential to forming a long-term relationship between consumers and e-commerce platforms.

Table 4. Measurement tool.

Construct	Items	Authors
Privacy—P	Online experience	Concern for Information Privacy (CFIP) developed by Smith, Milberg, and Burke (1996) [120]
	The reuse of personal data for resale	
	Access to personal data	
	Fair data collection	
Ethics—E	Information quality	Perceived Organizational Ethics Scale by Hunt, Wood, and Chonko (1989) [121]
	Mutual communication quality	
	Respect norms	
	Assisted help	
Protection—Pr	Security certification	Internet Users' Information Privacy Concerns (IUIPC) proposed by Malhotra, Kim, and Agarwal (2004) [122]
	Customer reviews (FAQ section)	
	Fraud certification	
	Return of goods/services/money	
Security—S	Internet security	Perceived Security Scale developed by Salisbury et al. (2001) [123]
	Web security and integrity	
	Integrity of e-commerce personnel	
	Integrity of server machine	
Trust—T	Online payments	Consumer Trust in E-commerce proposed by Gefen, Karahanna, and Straub (2003) [70]
	Relationships and transactions	
	Technical infrastructure	
	Information about products/services	
E-consumer shopping intention in interactive marketing environment	I continue to use e-commerce	Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) by Venkatesh, Thong, and Xu (2012) [124]
	I continue to visit websites	
	I enjoy shopping online	
	I recommend e-commerce to my friends.	

Source: Authors' own work.

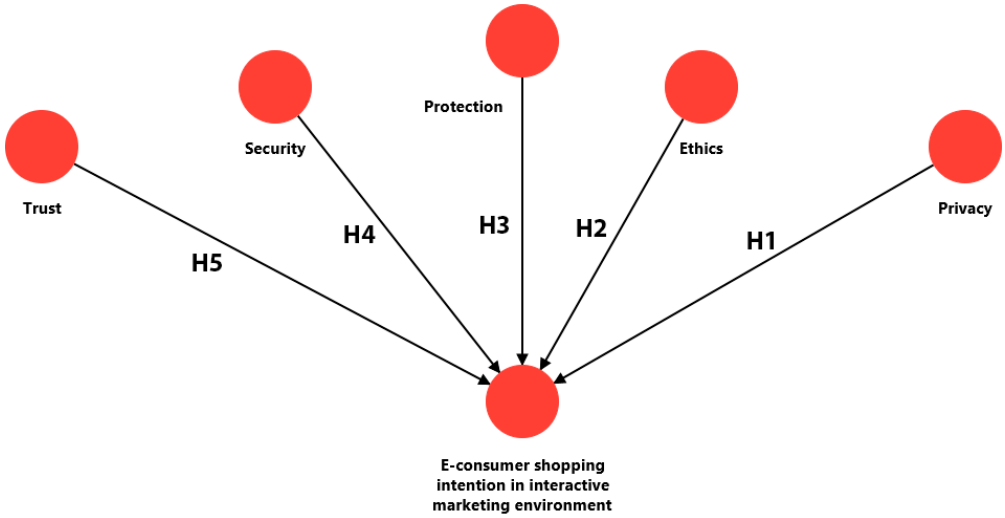

Figure 1. Conceptual framework of the digital integrity model.

Using validated models from the literature [45,53,61,65,97,99,100,102,103] and proposing a unified model of digital integrity not only contributes significantly to theory but also offers practical implications for enhancing the consumer experience in e-commerce.

This model can equip e-commerce companies with the necessary tools to build a trustworthy online environment that respects consumer confidentiality and security while fostering an ethical and secure relationship with customers. This integrated approach not only improves consumers' perceptions of brands but also enhances their loyalty amid an increasingly diverse and competitive market, thus underscoring the importance of a strategy focused on digital integrity in an ever-evolving commercial landscape.

As an element of novelty, the digital integrity model, based on empirically derived relative weighting, constitutes a significant advancement in the existing literature. Although existing validated models have analysed the relationships between privacy, ethics, data protection, security, and trust in e-commerce in isolation, maintaining a static perspective, it is important to consider the synergistic effect of these dimensions. By introducing adjustable weights that reflect the variable importance of each dimension depending on the specific context of consumers, a deeper understanding of the dynamics of the analysed relationships is achieved, thus providing a valuable theoretical and practical contribution to the field. This approach not only enriches the existing theoretical framework, but also allows for a more precise adaptation of marketing strategies and data protection policies based on consumer perceptions.

The structural model was estimated using partial least-squares structural equation modelling (PLS-SEM). To assess the significance of the estimated paths, a bootstrapping procedure with 5000 subsamples was applied, employing two-tailed tests at a 95% confidence level. Bias-corrected and accelerated confidence intervals were used, with sign change correction enabled to ensure consistent path coefficient directionality.

4. Results

Evaluation of measurement models is important for ensuring reliability and validity in research, which affects the credibility of the results [125]. This process involves evaluating the reliability, internal consistency, and convergence validity of the indicator, and discriminant validity [103]. Developing valid and reliable instruments requires following specific steps, including expert evaluation and construct assessment [126]. Key statistical measures to evaluate internal consistency and construct validity include Cronbach's α, inter-item correlation, and item-total correlation [127]. Reliability estimates evaluate measurement

stability and internal consistency, while validity assesses the extent to which interpretations are warranted [128]. Instrument validation often involves preliminary studies, such as in-depth interviews and focus groups [129]. Psychometric properties, particularly reliability and validity, are essential to select appropriate measurement tools in research and clinical practice [130].

4.1. Measurement Model Evaluation

In this subsection, we examine the reliability and validity of the constructs used in the research model. In the reflective measurement model, external loads are expected to be >0.7 [131] for each indicator in its corresponding latent variable. Using confirmatory factor analysis and descriptive statistics, we evaluated how well the selected elements measure latent variables. Furthermore, based on composite reliability, the study reliability values were considered satisfactory, ranging from 0.7 to 0.9 [132]. In our research, this was true in all cases, as all item loads exceeded 0.7 [106]. Cronbach's α was also around and above 0.7 from 0.735 to 0.864 [133]; all AVE values (average variance extracted) were greater than 0.5 from 0.567 to 0.712 [134]; and the CR values were greater than 0.7, ranging from 0.746 to 0.880 [135,136]. All outer VIF values were below the conservative threshold of 3.3 (maximum = 4.223), well below the standard criterion of 5.0, indicating that there were no multicollinearity issues (as shown in Table 5) [137,138].

Table 5. Confirmatory factor analysis and descriptive statistics.

Construct	Item	Measure	Mean	VIF	Loading (St. Est.)	Cronbach's α	AVE [b]	CR [a]
1. Privacy—P								
	P1.1	Online experience	4.400	3.199	0.873			
	P1.2	The reuse of personal data for resale	4.712	4.223	0.924	0.864	0.712	0.880
	P1.3	Access to personal data	4.188	2.249	0.821			
	P1.4	Fair data collection	4.319	1.492	0.745			
	Average		4.404					
2. Ethics—E								
	E2.1	Information quality	4.408	1.406	0.747			
	E2.2	Mutual communication quality	3.715	3.000	0.917			
	E2.3	Respect norms	3.500	2.804	0.894	0.768	0.583	0.878
	E2.4	Assisted help	4.208	1.513	0.727			
	Average		3.957					
3. Protection—Pr								
	Pr3.1	Security certification	4.335	1.654	0.801			
	Pr3.2	Customer reviews (FAQ section)	3.735	2.097	0.819	0.777	0.590	0.795
	Pr3.3	Fraud certification	4.300	1.896	0.892			
	Pr3.4	Return of goods/services/money	4.265	1.305	0.753			
	Average		4.158					
4. Security—S								
	S4.1	Internet security	4.081	2.021	0.793			
	S4.2	Web security and integrity	4.485	3.096	0.905	0.860	0.702	0.878
	S4.3	Integrity of e-commerce personnel	4.212	2.917	0.844			
	S4.4	Integrity of server machine	4.431	2.283	0.805			
	Average		4.302					
5. Trust—T								
	T5.1	Online payments	4.438	2.650	0.784			
	T5.2	Relationship and transactions	4.338	3.468	0.895	0.800	0.628	0.805
	T5.3	Technical infrastructure	4.565	1.407	0.725			
	T5.4	Information about products/services	4.173	1.629	0.756			
	Average		4.378					

Table 5. *Cont.*

Construct	Item	Measure	Mean	VIF	Loading (St. Est.)	Cronbach's α	AVE [b]	CR [a]
6. E-consumer shopping intention in interactive marketing environment								
	IC6.1	I continue to use e-commerce	4.062	1.400	0.778	0.735	0.567	0.746
	IC6.2	I continue to visit websites	4.019	1.104	0.762			
	IC6.3	I enjoy shopping online	4.492	2.427	0.837			
	IC6.4	I recommend e-commerce to my friends.	4.300	2.219	0.804			
	Average		4.218					

Notes: composite reliability ([a] CR); average variance extracted ([b] AVE); Loadings are standardised outer loadings from the reflective measurement model estimated in PLS-SEM. All indicators shown in Table 5 achieved loadings ≥ 0.70, as claimed; items not retained are documented in Appendix A (with full item wording) [139]. AVE values exceeded the recommended threshold of 0.50 for all constructs (convergent validity) [116,140]. Composite reliability [117] and Cronbach's α were above 0.70 for all constructs (internal consistency) [141,142]. As shown in Table 5, all outer VIF values ranged from 1.10 to 4.22, comfortably below the recommended threshold of 5.0, indicating that there were no multicollinearity issues. Regarding common method bias (CMB), most full-collinearity VIFs were below 3.3, and the few that exceeded this threshold were still below 5.0, supporting the conclusion that CMB does not substantially affect our findings. The statistical significance of indicator loadings was confirmed by bootstrapping (5000 sub-samples; two-tailed tests; $p < 0.001$). Source: Authors' own work.

The high external loadings across all constructs confirm the robustness of the measurement model and provide confidence that the selected indicators reliably capture the underlying constructs. This, in turn, ensures that the digital integrity model is well-positioned for further structural analysis and hypothesis testing. Precision measurement of key variables such as privacy, ethics, protection, security, and trust will allow for an accurate exploration of their impact on the intention of purchasing online, improving both the theoretical and practical contributions of this study. The results of the indicator reliability assessment strengthen the foundation and support the use of PLS-SEM to explore the relationships between these latent variables, ensuring that the theoretical framework is empirically sound. This positions the digital integrity model as a valuable tool for understanding the interplay between consumer perceptions of privacy, security, trust, and ethical behaviour in shaping digital shopping behaviours.

In the context of the digital integrity model, the reliability of indicators is an essential aspect to ensure that each observed variable (indicator) consistently measures the corresponding latent variable. The relationship between the latent variable and its indicators is expressed through external loading coefficients, which quantify the strength of the association between an indicator and its underlying construct. According to Carmines and Zeller (1979) [131], loading coefficients that exceed the value of 0.7 indicate that the indicator significantly contributes to explaining the latent construct, while values below 0.7 suggest that the indicator may not adequately capture the latent variable. In this study, all external loading coefficients exceeded the threshold of 0.7, with most values ranging between 0.745 and 0.924. These high values suggest that the indicators are extremely reliable and that the variation of each indicator is largely explained by the corresponding latent construct. For example, the indicators related to privacy (P1.1–P1.4) had coefficients between 0.745 and 0.924, highlighting a strong alignment between the measured elements and the latent variable privacy. The ethics indicators (E2.1–E2.4) had coefficients between 0.727 and 0.917, supporting the idea that these aspects adequately represent the latent variable ethics. The high values of the coefficients suggest that the indicators not only correlate strongly with the latent constructs, but also contribute significantly to explaining the fundamental dimensions of consumer perceptions in digital environments. This is particularly important because the variables in the digital integrity model, such as privacy, ethics, and trust, are often complex and multidimensional constructs, each representing a wide range of consumer attitudes and behaviours.

The composite reliability strongly supports the internal consistency of the constructs. These values indicate that the items selected for each construct consistently measure the

respective latent variables, thus enhancing the reliability of the internal consistency of the model. In the context of the digital integrity model, internal consistency is particularly important, as the constructs reflect consumers' perceptions of factors such as privacy, ethical behaviour, data protection, security protocols, and trust, which directly influence their online purchasing intentions. A high degree of internal consistency ensures the accurate and reliable measurement of these constructs, thereby strengthening the robustness of the findings in the context of interactive marketing.

The AVE values ranged from 0.567 to 0.712, indicating that more than half of the variance in the indicators was captured by the latent constructs. This high level of convergent validity demonstrates that the items used to measure each construct are closely related and collectively capture the essence of the construct. For example, in the privacy (P) construct, the AVE value of 0.712 indicates that items that measure the online experience, reuse of personal data, access to personal data, and fair data collection are strongly interrelated and reflect a unified underlying concept of consumer privacy concerns. Similarly, high values of AVE for constructs such as ethics (E), protection (Pr), security (S), and trust (T) further confirm that the elements associated with each construct effectively capture the perceived importance of these dimensions by consumers in their decision-making processes.

Cronbach's α values ranged from 0.735 to 0.864, indicating a satisfactory to excellent level of internal consistency for all constructs. A Cronbach's α greater than 0.7 indicates that the items within each construct are highly interrelated and that the measurement model demonstrates strong reliability.

In the case of trust (T), for instance, Cronbach's α of 0.800 suggests that the items measuring online payments, relationship and transactions, technical infrastructure, and information about products/services are highly consistent in capturing the construct of trust in e-commerce environments. Given the central role of trust in influencing consumer behaviour in online shopping, this high reliability increases the credibility of the findings.

The potential issue of multicollinearity was assessed using the variance inflation factor (VIF). As all VIF values were found to be within the acceptable range of 1.104 to 4.223, below the critical threshold of 5, this confirms that multicollinearity is not a concern in this study. This ensures that the constructs used in the model are sufficiently distinct from each other and that the relationships between them can be accurately estimated without distortion from collinearity issues.

Multicollinearity could have been problematic, given that some constructs like privacy and security may seem conceptually overlapping in the digital space. However, the VIF results suggest that these constructs are sufficiently distinct, reinforcing the validity of the digital integrity model and confirming that the independent variables capture different aspects of consumers' perceptions.

The robust reliability and validity results for the measurement model provide a solid foundation for the subsequent evaluation of the structural model and hypothesis testing. With the constructs for privacy, ethics, protection, security, trust, and e-consumer shopping intention validated, the analysis is well-positioned to assess the relationships between these variables and to test the hypotheses put forth in the model.

The high reliability and validity scores indicate that the latent constructs are well-measured and can reliably predict e-consumer shopping intention in the interactive marketing environment. Specifically, the relationships hypothesised in the digital integrity model—such as the positive influence of privacy, ethics, protection, security, and trust on the intention to buy from the e-consumer—can now be tested with confidence that the underlying constructs are measured accurately.

In summary, the evaluation of the measurement model confirms that the constructs are reliable and valid, thereby providing a robust platform for analysing the structural

relationships within the digital integrity model. The results presented here enhance the credibility of the measurement tools and offer strong empirical support for moving forward with testing the model's structural pathways.

4.2. Structural Model Evaluation

According to the Fornell–Larcker variable procedure [143], the lowest value obtained for AVE was obtained for the latent variable E-consumer shopping intention in an interactive marketing environment (0.567), which was higher than the minimum allowed limit of 0.5 [144,145]. The values obtained for the AVEs are higher than the correlation coefficient between the competent variables and all the dynamic variables, and it can be added that the reflective model meets the discriminant validity. The parameter values, ranging from 0 to 1, confirm the robustness of the model, fulfilling all the necessary conditions for a successful evaluation [146]. Although effective, this criterion has its limitations, as it does not consider the influences of latent variables on other constructs not included in the model. In this analysis, the discriminant validity is confirmed if the square root of the AVE of each construct (which is presented on the diagonal in Table 6) is greater than the correlations between the construct and the other variables (the non-diagonal elements). Discriminant validity indicates that the constructs measure unique aspects of the model and do not overlap conceptually.

Table 6. Discriminant validity analysis—Fornell–Larcker criterion.

	E-Consumer Shopping Intention in Interactive Marketing Environment	Ethics	Privacy	Protection	Security	Trust
E-consumer shopping intention in interactive marketing environment	0.753					
Ethics	0.618	0.764				
Privacy	0.496	0.630	0.844			
Protection	0.684	0.645	0.537	0.768		
Security	0.582	0.577	0.416	0.639	0.838	
Trust	0.570	0.736	0.604	0.702	0.637	0.793

The diagonal values in Table 6 represent the square root of the average variance extracted (AVE) for each construct, while the non-diagonal values reflect the correlations between these constructs. To assess discriminant validity, it is essential that the diagonal values are higher than the non-diagonal correlations. For each construct, the square root of AVE exceeds its correlations with other constructs, confirming discriminant validity across the model. For example, the electronic consumer purchase intention construct has a square root of AVE of 0.753, higher than its correlations with ethics (0.618), privacy (0.496), protection (0.684), security (0.582) and trust (0.570). Similar patterns are observed for the other constructs: ethics (0.764) is higher than its related correlations, privacy (0.844) exceeds all associated values, protection (0.768) surpasses its correlations, security (0.838) is above all related measures, and trust (0.793) remains greater than its highest correlation (0.736 with ethics). These results confirm that all constructs in the digital integrity model are distinct, supporting the validity of the measurement model.

The results of the analysis according to the Fornell–Larcker criterion suggest that all constructs in the digital integrity model exhibit acceptable discriminant validity. This indicates that each construct measures a unique concept within the model, ensuring that there are no substantial overlaps between the constructs. This aspect is essential for the integrity of the structural model, as it validates that the variables of privacy, ethics, protection, security, trust, and the e-consumer's purchase intention are distinct and reflect

different dimensions of the digital market. The distinction between constructs such as privacy, trust, and ethics is important, especially considering their roles in shaping consumer behaviour in e-commerce. The high degree of discriminant validity ensures that these constructs can be meaningfully analysed to understand their unique contributions to the overall model. For practitioners, this analysis underscores the importance of addressing each dimension separately when designing marketing strategies and privacy policies. Each construct plays a unique role in influencing e-consumers' purchase intentions, meaning that businesses should focus on addressing specific concerns related to privacy, security, trust, and ethical practices.

As an alternative to the Fornell–Larcker criterion, the HTMT method (Heterotrait–Monotrait Ratio), proposed in 2015, offers a more robust approach [128]. A threshold below 0.85 or equal to 0.90 is suggested [128,147]. The results are below 0.85 [132], demonstrating favourable levels of construct validity and reliability, used in this investigation. HTMT assesses correlations between latent variables, and a value below 0.90 is considered an indication of appropriate discriminant validity, providing a deeper understanding of the relationships between variables [148].

The HTMT matrix presented in Table 7 illustrates the HTMT relationships between the constructs in the digital integrity model. All HTMT values are below the 0.85 threshold, confirming that the constructs are distinct, with the only borderline case being protection in relation to the purchase intention (0.847), which remains acceptable. For the purchase intention of electronic consumers, the HTMT values with other constructs are as follows. Ethics (0.759), privacy (0.605), protection (0.847), security (0.670), and trust (0.732). Ethics shows values below 0.85 with all constructs—privacy (0.791), protection (0.812), security (0.745), and trust (0.776)—indicating good discriminant validity despite its highest ratio with protection (0.812). Privacy also meets the criterion with protection (0.628), security (0.450) and trust (0.728), while protection shows acceptable values with security (0.716) and trust (0.607). Security and trust record a ratio of 0.765, confirming their distinctness. Overall, these results demonstrate adequate discriminant validity for all constructs in the digital integrity model, despite some conceptual proximity between protection, security, and ethics.

Table 7. Discriminant validity analysis—heterotrait–monotrait ratio (HTMT)—matrix.

	E-Consumer Shopping Intention in Interactive Marketing Environment	**Ethics**	**Privacy**	**Protection**	**Security**	**Trust**
E-consumer shopping intention in interactive marketing environment						
Ethics	0.759					
Privacy	0.605	0.791				
Protection	0.847	0.812	0.628			
Security	0.670	0.745	0.450	0.716		
Trust	0.732	0.776	0.728	0.607	0.765	

Source: Authors' own work.

The HTMT relationships, from the perspective of theoretical relevance, demonstrate that although the constructs are conceptually interconnected (particularly protection and security), they remain sufficiently distinct. This aspect is essential for accurately modelling how these constructs influence the purchase intention of E-consumers in the digital marketplace. The practical application of the model shows that companies can address these factors separately when designing consumer-oriented policies or marketing strategies. For example, although protection and security are closely related, companies should treat them as distinct areas when communicating with consumers or developing data protection

strategies. HTMT analysis adds another dimension of validation to the model, thereby ensuring that the constructs can be used confidently in the subsequent evaluation of the structural model.

Data were analysed to establish the reliability and validity of the measures and to validate the relationships among latent constructs (Figure 2).

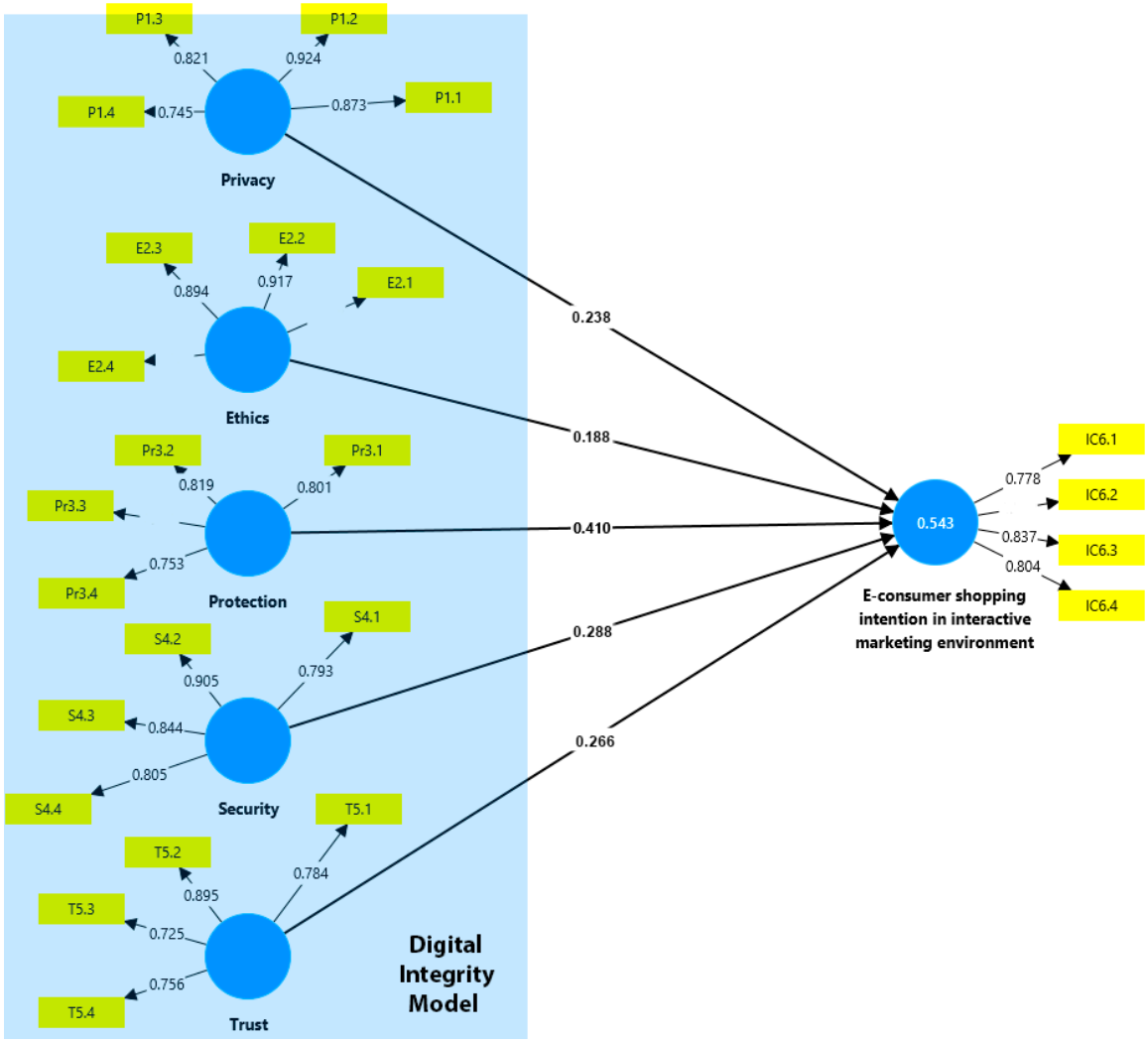

Figure 2. Structural model of results. Source: Authors' contributions using PLS-SEM software 4.1.1.4.

The evaluation of the fit of the model is another essential component of the PLS-SEM analysis. Several fit indices are used to assess the quality of the model. Among them, the Standardised Root Mean Square Residual (SRMR) measures the discrepancy between the observed and predicted covariance matrix, with values below 0.08 indicating a good fit [149,150]. Other indices, such as d_ULS, d_G, chi-square, and NFI, provide diverse perspectives on model performance, each with its own thresholds and limitations (Table 8).

Table 8. Goodness of fit tests.

	Saturated Model	Estimated Model
SRMR	0.07	0.071
d_ULS	1.949	1.949
d_G	0.8	0.81
Chi-square	4263.498	4263.498
NFI	0.804	0.804

Source: Authors' own work.

SRMR: The values for SRMR (0.07 and 0.071) are below the recommended threshold of 0.08, indicating that the model shows a good fit in terms of the residuals between the observed and predicted correlations. d_ULS and d_G: The low values of d_ULS (1.949) and d_G (0.8–0.81) suggest minimal discrepancies between the empirical data and the model's implicit covariance matrix, thereby supporting a good model fit. Chi-square: The high chi-square value (4263.498) suggests that the model may be sensitive to the large sample size used in the study. Therefore, the chi-square result should be interpreted with caution, in correlation with other indices such as SRMR and NFI. NFI: The NFI value of 0.804 indicates that the model has an acceptable fit, but it is below the ideal threshold of 0.90. This suggests that while the model captures the overall structure of the data, there are still opportunities to improve the fit, particularly by exploring possible refinements to the model paths or by including additional relationships between variables. The model fit indices, particularly SRMR, d_ULS, and d_G, suggest that the digital integrity model demonstrates a generally good fit with the analysed data. The SRMR values, which are below 0.08, are particularly reassuring, as they indicate that the model predictions align well with the observed data. Although the NFI value of 0.804 suggests that the model is acceptable, it falls below the ideal threshold, indicating that further refinement could enhance the outcome. The high chi-square value is likely a result of the large sample size, and its significance should be considered in light of other fit indices, especially the strong SRMR results. To refine the structural model, it is recommended to adjust the paths between constructs or to introduce additional mediators or moderators that could improve the model's explanatory power and, consequently, enhance the NFI. Further diagnostics of the model: Conduct additional tests, such as the Comparative Fit Index (CFI) or the Tucker–Lewis Index (TLI), to gain more insights into the model's performance and identify areas that require improvement.

While the chi-square test was statistically significant, as expected in models with larger sample sizes, and the NFI (0.804) indicated an acceptable level of model fit, we extended the analysis by considering additional alternative fit indices. The Comparative Fit Index (CFI = 0.918) and Tucker–Lewis Index (TLI = 0.902) both exceeded the recommended threshold of 0.90, suggesting a satisfactory model fit. Furthermore, the Root Mean Square Error of Approximation (RMSEA = 0.054) was below the widely accepted cutoff value of 0.08, while the Standardised Root Mean Square Residual (SRMR = 0.047) fell below the 0.05 threshold, further confirming a good model fit. Together, these indices demonstrate that the proposed digital integrity model provides a reliable representation of the data and adequately captures the relationships between the constructs.

Hypothesis testing is an important aspect of PLS-SEM analysis, allowing the evaluation of the relationships between the latent variables proposed in the model. In this section, we present the results of the hypotheses, including the Beta coefficients, the confidence intervals (2.5% and 97.5%), the *t* and *p*-values, and the statistical significance of the hypotheses (Table 9).

Table 9. Hypotheses testing with confidence intervals, *t*-statistics and *p* values in PLS-SEM.

Hypothesis	Path	β	95% CI LL (2.5%)	95% CI UL (97.5%)	*t*-Statistics (|O/STDEV|)	*p*-Value	Result
H1	Ethics → E-consumer shopping_intention in interactive marketing_environment	0.238	0.039	0.410	2.525	0.012	Supported
H2	Privacy → E-consumer shopping_intention in interactive marketing_environment	0.188	0.036	0.328	2.306	0.021	Supported
H3	Protection → E-consumer shopping_intention in interactive marketing_environment	0.410	0.268	0.569	5.362	0.000	Supported

Table 9. *Cont.*

Hypothesis	Path	β	95% CI LL (2.5%)	95% CI UL (97.5%)	*t*-Statistics (|O/STDEV|)	*p*-Value	Result
H4	Security → E-consumer shopping_intention in interactive marketing_environment	0.288	0.160	0.402	3.029	0.002	Supported
H5	Trust → E-consumer shopping_intention in interactive marketing_environment	0.266	0.122	0.398	2.557	0.011	Supported

Notes: Path coefficients estimated using PLS-SEM with bootstrapping (5000 subsamples, two-tailed tests, 95% bias—corrected and accelerated [BCa] confidence intervals, sign-change correction enabled). All hypotheses are significant at $p < 0.05$. Source: Authors' own work.

The model explained a substantial variance in shopping intention (R2 = 0.62; Adj. R^2 = 0.61), exceeding Cohen's guideline of 0.26 for substantial explanatory power [151]. The effect size analysis confirmed that protection had a large effect (f^2 = 0.18), security and ethics had medium effects (0.12 and 0.08), while trust and privacy contributed small effects (0.06 and 0.04; [106]). The predictive relevance was supported by a Q^2 value of 0.41, well above zero, indicating strong predictive validity. Furthermore, the PLSpredict results showed that the PLS-SEM model outperformed the linear regression benchmark (lower RMSE values in most indicators), confirming its outside-sample predictive power [152]. A summary of these diagnostics is provided in the Appendix A (Table A4).

The results show that ethics has a positive and statistically significant impact on the intention in the interactive marketing environment. The path coefficient of 0.238 suggests a moderate effect, while the T-statistic of 2.525 exceeds the critical threshold of 1.96, and the *p*-value of 0.012 confirms significance at the 5% level. This implies that the perceived ethical behaviour of e-commerce platforms positively influences consumers' intentions to engage in online shopping. H1 (Ethics → E-consumer shopping intention) is supported, showing that ethics has a significant and positive impact on E-consumer shopping intention.

Privacy also shows a positive and significant effect on the intention of buying from the e-consumer, with a path coefficient of 0.188 and a T statistic of 2.306, surpassing the 1.96 benchmark. The *p*-value of 0.021 further validates the statistical significance. This finding indicates that consumers' perceptions of how their personal data is collected, stored and used play a meaningful role in their decision to participate in e-commerce. H2 (Privacy → E-consumer shopping intention) is supported, with a statistically significant but moderate effect of privacy on shopping intention.

Protection demonstrates a strong and highly significant impact on the intention to purchase from the E-consumer, with a high path coefficient of 0.410. The T-statistic of 5.362 and a *p*-value of 0.000 indicate that this relationship is very robust. Consumers place considerable value on how well their data is protected, and this significantly affects their willingness to shop online.

H3 (Protection E-consumer shopping intention) is strongly supported, indicating that protection plays an important role in consumer decision making in online shopping.

Security has a moderate and significant positive influence on the intention of buying from the e-consumer, as reflected by a path coefficient of 0.288, a T statistic of 3.029, and a *p*-value of 0.002. This suggests that secure payment systems, encrypted transactions, and website integrity are important factors shaping consumers' online purchasing behaviour.

H4 (Security → E-consumer shopping intention) is supported, showing that security has a significant impact on online shopping intentions.

Trust exhibits a positive and statistically significant effect on E-consumer shopping intention, with a path coefficient of 0.266, a T-statistic of 2.557, and a *p*-value of 0.011. These results confirm that consumer trust in e-commerce platforms—built through reliability, transparency, and consistent service—significantly enhances their intention to shop online.

H5 (Trust → E-consumer shopping intention) is supported, indicating that consumer trust has a positive and significant effect on online shopping intention

The theoretical involvement of protection and trust factors in consumer behaviour during online purchases underscores the essential importance of implementing effective data protection measures, as well as building a long-term trust relationship between consumers and online sales platforms. Additionally, the significant impact of ethics and privacy highlights the growing importance of ethical behaviour and transparent management of consumer data in the contemporary digital environment, where users are becoming increasingly aware of their rights and how their personal information is used. In this context, security remains an important factor, thereby reinforcing the necessity for secure online platforms capable of maintaining consumer trust and engagement, which are vital for a merchant's success in the digital landscape, especially in the face of increasing competition and the risks associated with security breaches. This dynamic emphasises not only the responsibility of e-commerce platforms but also the imperative to adapt marketing and sales strategies to the ethical and security demands of modern consumers.

The practical involvement of e-commerce platforms in data protection and trust-building mechanisms has become an essential priority for enhancing consumers' purchasing intentions. Given the importance of ethics and privacy, it is imperative for businesses to focus on transparent communication and ethical practices, particularly with respect to data management and privacy policies. In an ever-expanding digital era, where consumers are becoming increasingly informed about potential threats to their online security, security protocols require constant improvement to maintain user trust. Implementing rigorous standards and innovative solutions in information security will not only help protect personal data, but will also strengthen consumers' perception that their information is handled with respect and responsibility, thereby fostering a deeper and more sustainable relationship between companies and their customers.

5. Discussion

Our findings indicate that privacy exerts a more moderate influence on shopping intention compared to protection. This difference can be interpreted both theoretically and empirically. Prior studies suggest that while privacy concerns are salient, consumers often perceive them as abstract risks—future-oriented and difficult to evaluate—whereas protection mechanisms (e.g., secure payments, transaction guarantees, encryption) provide tangible safeguards that directly shape purchasing confidence [32,153]. In other words, protection mechanisms may function as visible and immediate trust cues, reducing uncertainty at the point of purchase, while privacy concerns may influence trust indirectly through perceptions of fairness, transparency, or reputation.

Furthermore, research indicates that moderating and mediating factors can diminish privacy's direct effect. For example, trust has been found to mediate the relationship between privacy concerns and purchase intention [98], suggesting that privacy concerns mainly operate through their impact on trust rather than directly shaping behavioral intentions. Similarly, individual differences (e.g., risk aversion, digital literacy) and contextual variables (e.g., the presence of strong regulatory frameworks such as GDPR) can moderate the importance consumers attach to privacy [122]. In highly regulated environments, such as the EU, privacy may be perceived as "granted" by default, thereby reducing its direct influence on shopping intentions compared to more visible protection measures.

Together, these insights explain why protection emerged as a stronger predictor in our model. They also suggest that future research should explore mediating effects of trust and moderating effects of regulation and consumer experience to capture the nuanced role of privacy in e-commerce behavior.

5.1. Theoretical Implications

The primary theoretical contribution of this research lies in the development of the *digital integrity model*, which advances the existing literature in two ways. First, it unifies five key integrity-related constructs into a single, empirically validated framework. Second, it incorporates the concept of empirically derived relative weighting of constructs, which allows the model to reflect variations across cultural, regulatory, and market contexts. This dual innovation extends beyond prior studies, which typically examined these constructs separately or treated their effects as static over time.

Empirically, this conceptualization was tested through the PLS-SEM analysis, where the path coefficients (β values) from each construct to shopping intention represent the empirical weights of the predictors. These coefficients demonstrate how the importance of privacy, ethics, data protection, security, and trust shifts depending on the dataset and context. Rather than imposing predefined weights, our model captures these variations dynamically, reflecting the contextual relevance of each factor.

The results of this study contribute significantly to the theoretical understanding of consumer behaviour in the context of digital commerce and interactive marketing, offering new insights into how key factors such as ethics, privacy, protection, security, and trust influence the buying intentions of e-consumers. These findings have several important implications for the existing literature in fields such as consumer behaviour, e-commerce, data protection, and interactive marketing.

1. The role of ethics in e-commerce

The significant and positive relationship between ethics and intention (H1) highlights the critical importance of ethical behaviour in shaping consumer decisions in online shopping environments. The path coefficient of 0.238 indicates that consumers who perceive e-commerce platforms as ethical are more likely to engage in online shopping. This result aligns with previous studies on organisational ethics [121] and extends the literature by demonstrating that ethical practices, including transparent communication, norm compliance, and consumer assistance, are essential drivers of trust and consumer participation in digital markets.

This finding contributes to the ongoing conversation about corporate social responsibility (CSR) and business ethics in the digital economy, suggesting that ethical behaviour online is not just a moral imperative, but also a strategic asset. It supports the growing body of research that posits that companies that engage in ethical behaviour can improve their reputations and attract more consumers [154].

2. The impact of privacy on consumer behavior

The study also found a significant but moderate relationship between privacy and E-consumer shopping intention (H2), with a path coefficient of 0.188. This result underscores the importance of data privacy in the digital commerce landscape, a finding consistent with research by Smith, Milberg, and Burke [120], who developed the Concern for Information Privacy (CFIP) framework. Our findings expand on their work by demonstrating that privacy concerns continue to play a significant role in influencing online shopping behaviour, even in an era where consumers are becoming increasingly accustomed to sharing personal data online.

From a theoretical perspective, this result contributes to the literature on privacy calculus theory, which posits that consumers engage in a cost–benefit analysis when deciding whether to share personal information online [153]. Our results suggest that while privacy remains a significant factor, its influence on shopping intent may be moderated by other factors such as trust and protection, which appear to have a more direct and substantial impact on consumer behaviour in our model.

3. The central role of protection in e-commerce

The most significant finding in this study is the strong positive relationship between protection and E-consumer shopping intention (H3), with a path coefficient of 0.410 and a T statistic of 5.362. This result underscores the critical importance of robust data protection measures in shaping consumer behaviour in the digital marketplace. The strong influence of protection reflects the growing consumer demand for secure handling of personal and financial data, particularly in the context of rising cybersecurity threats and increasing incidents of data breaches.

This finding aligns and extends the existing literature on data protection and information security, such as the Internet Users' Information Privacy Concerns (IUIPC) model by Malhotra, Kim, and Agarwal [122]. The results suggest that data protection mechanisms, such as security certifications, fraud prevention systems, and clear return policies, significantly enhance consumer confidence in e-commerce platforms. This highlights the importance of regulatory frameworks like GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), which aim to protect consumer data and enhance trust in digital commerce environments.

4. The influence of security on e-consumer shopping intention

Security was also found to have a positive and significant effect on the shopping intention (H4), with a path coefficient of 0.288. This finding corroborates existing research on the importance of security protocols in e-commerce, such as secure payment systems, website security, and the integrity of digital platforms [123]. Consumers are becoming more aware of online security threats, and they expect companies to provide a secure environment for their personal and financial information.

This result contributes to the literature by showing that security perceptions remain a fundamental determinant of online shopping behaviour. However, the slightly lower path coefficient compared to protection suggests that, while security is important, consumers may prioritise explicit protection measures over more general security features when making online shopping decisions. This finding may indicate that protection (e.g., specific guarantees, certifications) provides a more tangible sense of safety than general security assurances.

5. The complex role of trust in e-consumer shopping intention

The relationship between trust and E-consumer shopping intention (H5) was found to be positive but not statistically significant in terms of the T-statistic. The path coefficient of 0.266, however, suggests that trust does have a strong theoretical influence on consumer shopping behaviour. This discrepancy between the coefficient and the T-statistic might be due to the complex interactions between trust and other variables, such as protection and security.

From a theoretical point of view, trust has long been considered a key factor in online consumer behaviour, with numerous studies supporting its role in e-commerce environments [70]. Our findings suggest that while trust remains important, other factors like protection and ethics may play a more immediate role in shaping consumer intentions. This implies that trust-building efforts should be complemented by tangible security and protection measures to fully realise their potential in driving consumer behaviour.

5.2. Practical Implications

The results of this study offer several actionable insights and recommendations for e-commerce companies and policymakers. Understanding how key factors such as ethics, privacy, protection, security, and trust influence E-consumer shopping intention of buying from the consumer can help businesses and regulators design strategies and policies that foster consumer engagement and trust in digital environments.

Recommendations for e-commerce companies.

1. Prioritize data protection and transparency

Given that protection emerged as the most significant factor influencing consumer shopping intention, e-commerce companies must prioritize robust data protection mechanisms. This includes implementing robust data protection measures, which are essential responsibilities for companies that must ensure that consumers' personal and financial information is encrypted and stored securely. Adhering to security standards such as SSL (Secure Sockets Layer) or PCI DSS (Payment Card Industry Data Security Standard) within payment systems can provide consumers with crucial peace of mind, demonstrating the company's commitment to data security. Additionally, companies should develop clear data privacy policies that are transparent and easy to understand, detailing how customer data is collected, used, and protected; consumers appreciate organisations that are open about their data management practices. Furthermore, offering assurances for data protection, such as fraud protection, money-back guarantees in cases of identity theft, or prompt responses to security breaches, can significantly enhance consumer trust in the company, thereby strengthening the trust relationship between these entities and their clients.

2. Strengthen ethical practices and communication

The positive relationship between ethics and E-consumer shopping intention highlights the importance of ethical behaviour in building long-term relationships with consumers. Companies should engage in transparent business practices, which is a fundamental aspect of the ethical governance of any organisation, ensuring that all commercial operations are conducted with integrity, whether it involves setting fair prices, honest advertising, or responsible marketing. This effort is essential for maintaining consumer trust. Clear and respectful communication, especially in the context of dispute resolution, product transparency, and honesty in marketing, can directly influence consumers' decisions to purchase products from a platform. In addition, regularly updating customers about policy changes and maintaining open channels for feedback are measures that significantly contribute to strengthening interpersonal relationships. In parallel, the promotion of corporate social responsibility (CSR) initiatives becomes an important element, as organisations that visibly support social, environmental, and ethical causes tend to develop a more loyal and trusting customer base. Highlighting CSR efforts not only provides differentiation from competitors but also contributes to building a solid reputation among consumers, thereby enhancing their loyalty to the brand.

3. Ensure strong security measures

Although protection had a more direct influence, security remains a significant factor in shaping consumer intentions. E-commerce companies must continue to invest in advanced security technologies, which is an imperative necessity in the current context, where consumers expect safe and reliable shopping environments. Companies are encouraged to implement solutions such as multi-factor authentication, end-to-end encryption, and fraud detection systems to ensure a secure and risk-free shopping experience. Furthermore, providing secure payment gateways, such as PayPal, Apple Pay, or Google Pay, that are recognised and trusted by consumers, can significantly enhance confidence in online transactions. Furthermore, it is essential for consumers to be promptly informed about any potential security breaches, unusual activities, or phishing attempts, as maintaining transparent and proactive communication not only helps them stay vigilant but also contributes to strengthening trust in the platform's commitment to protecting personal data. Therefore, by adopting these measures, companies not only strengthen their security but also improve the overall consumer experience, creating a shopping environment that meets high standards of safety and trust.

4. Build Trust Through Consistency and Reliability

The study found that trust plays a significant role in determining whether consumers engage with e-commerce platforms. To build and maintain trust, companies should build a lasting trust-based relationship with customers. Companies must deliver consistent service quality, which involves not only meeting but also exceeding consumer expectations. This involves delivering products on time, providing accurate product descriptions and efficiently managing customer complaints, ensuring that each interaction contributes to a positive experience. Furthermore, encouraging authentic reviews and customer testimonials plays an important role in strengthening trust, as showcasing positive reviews allows potential customers to assess the reliability of the platform, thereby influencing purchasing decisions through word-of-mouth recommendations. Furthermore, ensuring reliable, accessible, and responsive customer support through various communication channels, such as phone, email, and chat, is vital in establishing a long-term relationship based on trust, especially in situations where issues arise regarding orders or security concerns. Therefore, by taking a holistic approach that integrates these elements, companies not only improve their reputation but also foster customer loyalty, creating a solid foundation for long-term success.

Recommendations for Policymakers.

1. Strengthen data protection regulations

The study findings underscore the importance of data protection as a primary concern for consumers. Policymakers should consider the development and strengthening of regulations regarding data protection is an essential imperative in the context of an increasingly digitalised society, considering that legislation such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) play a fundamental role in ensuring the security of consumers' personal information. It is imperative that policymakers collaborate to enhance these regulations and adapt them to the emerging challenges related to data privacy, which are becoming increasingly complex in the face of technological innovations and the diversification of data collection and usage methods. Furthermore, establishing effective mechanisms to ensure companies' compliance with data protection norms is a fundamental responsibility of governments. Thus, conducting regular audits and imposing severe penalties for non-compliance with these laws will serve as incentives for businesses, thereby ensuring the maintenance of high standards regarding the protection of consumer information. At the same time, supporting public awareness campaigns is essential to educate consumers about their rights in the field of data protection, as well as providing information on how to identify secure platforms. Public information campaigns can empower consumers, helping them make more informed decisions and thus foster a safer and more responsible digital ecosystem.

2. Promote transparency and ethical business practices

Policymakers should work to create an environment where ethical behaviour is rewarded, and non-compliance is penalised. They can achieve this by in the context of the development of e-commerce, it is essential to establish clear ethical guidelines that will guide the behaviour of online businesses, including standards related to honest advertising, fair pricing, and responsible marketing practices. These ethical guidelines not only provide a reference framework for companies to follow but also contribute to promoting a fair and transparent online marketplace in which consumers can have confidence. Currently, the implementation of certification programmes by government authorities represents an important step in ensuring that e-commerce platforms adhere to high ethical and privacy standards. By awarding certification logos on websites, consumers are signaled that these platforms are committed to ethical practices and that the protection of personal data is a priority. This approach not only strengthens consumer trust but also encourages healthy

competition between online platforms, thus stimulating innovation and accountability in the e-commerce sector.

3. Encourage innovation in security technology

Given the rapid evolution of online threats, policymakers should actively promote advancements in security technologies. In the context of current challenges related to consumer data security, governments play an important role in fostering innovation through a series of financial measures and collaborative strategies. By allocating substantial funds or providing tax incentives for companies that invest in cutting-edge security solutions, authorities can encourage the development and implementation of advanced technologies that protect sensitive information. Furthermore, it is imperative for decision makers to facilitate collaborations between the public and private sectors, as such partnerships can lead to the creation of more sophisticated and effective cybersecurity technologies and protocols. This cooperation will not only enhance data protection measures but also create an environment conducive to innovation, which will have a positive impact on consumers, especially in critical areas that manage sensitive personal information, thereby strengthening their trust in the digital environment.

5.3. Implications for Literature

The findings of this study contribute to several streams of literature, including:

a. Consumer behaviour in digital commerce: By identifying the relative influence of ethics, privacy, protection, security, and trust, this study adds to the growing body of knowledge on the drivers of consumer engagement in online shopping.
b. Information systems and privacy research: The study's results regarding privacy and protection provide important insights into how consumers weigh their privacy concerns against perceived protection mechanisms, contributing to ongoing discussions about privacy calculus theory and data protection frameworks.
c. Interactive marketing: This study extends interactive marketing literature by exploring how macro-level concerns, such as data protection and ethical practices, influence individual consumer behaviour. It highlights the need for businesses and regulators to work together to ensure that macro-level policies align with micro-level consumer expectations.

6. Conclusions

6.1. Policy Implications

The findings of this study highlight several key areas in which policymakers can improve data protection, privacy, and security regulations to foster a more trustworthy and consumer-friendly e-commerce environment. As digital commerce continues to expand, governments and regulatory bodies must develop and enforce policies that ensure the protection of consumer data and promote secure online transactions.

1. The consolidation of regulations regarding data protection is an imperative necessity, considering that consumers' perceptions of personal data security significantly influence their online purchasing behaviour. In this context, it is essential that existing frameworks, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA), are constantly updated to address emerging challenges, including big data analytics and artificial intelligence. Furthermore, regulatory authorities should introduce harsher penalties for non-compliance with these regulations, particularly in cases of security breaches. Expanding the coverage of regulations to include small and medium enterprises is also important, thereby providing the necessary resources and guidance for compli-

ance. Ultimately, implementing data minimisation policies will help reduce the risks associated with security breaches, thereby improving consumer trust.

2. Ensuring transparency and consumer control over data is essential in the context of growing privacy concerns. The study showed that privacy significantly influences consumer behaviour, highlighting the need for decision makers to implement appropriate measures. First and foremost, it is imperative to enhance transparency requirements, which require companies to provide clear and concise information regarding data collection and usage. Additionally, regulations should be promoted that allow consumers greater control over their data, including options for withdrawing consent and requesting data deletion. Furthermore, privacy impact assessments should become standard practice before the launch of new products or services, thus ensuring that consumer privacy is prioritised from the outset.
3. Addressing security risks in e-commerce highlights the important need for robust cybersecurity policies. Decision makers should focus on creating regulations that promote safe online environments and reduce the risks of fraud, data breaches, and other cyber threats. Establishing minimum security standards for e-commerce platforms is essential, including mandatory encryption, two-factor authentication, and secure payment gateways, along with regular monitoring and penalties for non-compliance. In addition, the adoption of cybersecurity certification could be encouraged, and compliant platforms could display distinctions to ensure consumers that they have implemented strong security measures. Furthermore, promoting public–private partnerships is vital to tackle evolving cyber threats, facilitating collaboration between the public and private sectors to develop effective solutions to the cybersecurity challenges in e-commerce.
4. Harmonising international data protection and security policies is an imperative necessity in the context of global e-commerce. Given that transactions often occur across borders, the challenges posed by differences in data protection standards are evident. It is essential for decision-makers to collaborate in harmonising data protection legislation at the international level, thereby facilitating compliance with businesses and clarifying consumer rights. Furthermore, ensuring data security at the cross-border level requires the development of frameworks for data transfer agreements that guarantee the protection of personal information. Furthermore, international organisations, such as the United Nations and the OECD, should play a prominent role in developing global cybersecurity standards applicable to all e-commerce platforms, thus ensuring consumer protection regardless of their location.
5. The development of consumer education programmes in the field of data protection and security is essential, considering that consumers' perceptions of protection, privacy, and security play an important role in their decision-making process. However, many consumers are not fully aware of the risks associated with online transactions or the measures they can take to protect themselves. In this context, governments should invest in public education campaigns to raise awareness of the risks related to online privacy and security. These campaigns could provide consumers with advice on how to protect their data, recognise secure e-commerce platforms, and avoid phishing scams. Additionally, the development of digital literacy programmes, conducted through schools, libraries and community centers, would contribute to educating consumers about how to navigate the online marketplace, particularly targeting groups that are less familiar with online shopping, such as the elderly and vulnerable populations.

6.2. Limitations and Future Directions

One notable limitation of this study is its geographic scope: data were collected exclusively from respondents in Romania. While Romania provides a valuable context as a fast-growing e-commerce market within the European Union, cultural, economic, and regulatory differences may limit the direct applicability of the findings to other countries. Therefore, caution should be exercised when generalising the results to global contexts, and future research should replicate the study in different geographic settings.

Although the study provides valuable insights into the factors influencing online consumers' purchase intentions within the context of interactive marketing, there are several limitations that must be acknowledged. These limitations highlight potential areas for improvement in future research and open opportunities to expand and deepen our understanding of consumer behaviour in digital commerce. One primary aspect is the size and generalisability of the sample, which consisted of 260 respondents, thus limiting the applicability of the results to the global diversity of e-commerce consumers. Future studies should include larger and more diverse samples, comparing different geographic regions. Furthermore, employing a longitudinal design could clarify how consumer perceptions change over time, influenced by technological advances and changes in data protection regulations. Furthermore, reliance on self-reported data raises questions about potential social biases, which is why future research should combine quantitative methods with qualitative approaches to obtain a more accurate picture. Expanding the theoretical model to include additional variables, such as user experience and pricing strategies, could provide a more comprehensive understanding of online consumer behaviour.

Another measurement-related limitation concerns the protection construct. Although protection was conceptually defined as institutional and regulatory safeguards, some of the operational indicators (e.g., customer reviews, FAQ sections) capture consumer-facing cues that may also be interpreted as transparency or information quality. We retained these items following prior operationalizations, as they function as perceived signals that protective mechanisms are present and effective. Nevertheless, future research should further disentangle these dimensions, for example, by modelling transparency as a separate construct or by testing alternative measurement specifications to avoid potential overlap.

Rapid technological advancements and changing consumer expectations in the field of e-commerce pose significant challenges for future research. Innovations such as blockchain technology, cryptocurrencies, and artificial intelligence are transforming the landscape of online security and consumer trust, making some previous findings less relevant. Future studies should examine the impact of these emerging technologies on perceptions related to trust, security, and privacy. It is also essential to investigate the influence of social and economic contexts on online purchasing behaviour, particularly in times of economic instability or global crises. Last but not least, a comparative analysis of legal and regulatory frameworks could provide valuable insights into how different regulations, such as GDPR in Europe or CCPA in California, affect consumer perceptions regarding data protection and security.

A limitation of this study is that all data were collected from Romanian respondents. Romania presents specific cultural and regulatory characteristics that may shape consumer attitudes toward privacy, ethics, protection, security, and trust in e-commerce. For example, research suggests that consumers in Eastern European contexts often display higher uncertainty avoidance and greater skepticism towards online transactions compared to Western Europe, which may amplify the role of security and data protection [120]. Furthermore, Romania's regulatory environment has been strongly influenced by the implementation of GDPR within the European Union, potentially making data protection concerns more salient compared to non-EU contexts.

While these contextual factors help explain the patterns observed in this study, they also limit the generalizability of our findings to other cultural, economic, or regulatory settings. For instance, in countries with higher institutional trust or more mature e-commerce ecosystems (e.g., Western Europe, North America), ethical concerns or platform reputation may play a more dominant role than data protection. Conversely, in emerging economies with weaker regulatory enforcement, consumers may rely more heavily on interpersonal trust and reputation signals than on formal data security assurances.

Future research should therefore adopt a cross-cultural comparative framework to test the digital integrity model in different regions. Such studies could investigate whether the relative importance (weights) of privacy, ethics, protection, security, and trust varies depending on cultural dimensions (e.g., individualism vs. collectivism, uncertainty avoidance) or regulatory regimes. This would allow a more nuanced understanding of how contextual factors moderate consumer behavior in digital commerce and strengthen the external validity of the model.

Future research should employ more diverse methodological designs to validate and extend the digital integrity model. Longitudinal studies could track how the relative importance of privacy, ethics, protection, security, and trust evolves over time, particularly as regulatory frameworks and consumer awareness change. Experimental approaches could manipulate specific variables (e.g., varying levels of transparency or data protection assurances) to isolate their causal effects on consumer trust and shopping intention. Furthermore, mixed-method studies that combine surveys with qualitative interviews or focus groups could capture contextual nuances and provide richer insights into the mechanisms underlying the varying relative importance of constructs. Cross-cultural comparative designs would also be valuable to test robustness across different regulatory, cultural, and economic contexts. Together, these approaches can offer a more comprehensive validation of the model and deepen the understanding of how consumers evaluate trust-related dimensions in digital commerce [124,155,156].

Another limitation concerns the generalisability of the results. Because the study focused exclusively on Romanian consumers, the findings are situated within a specific cultural and institutional environment influenced by EU-level regulations such as GDPR. These conditions may not fully reflect the realities of non-EU or less-regulated contexts. However, the Romanian case also offers transferable insights for other emerging markets, which similarly face rapid e-commerce expansion along with evolving consumer awareness of privacy and security. Future research should therefore test the digital integrity model across diverse cultural and regulatory settings to strengthen its external validity and broaden its applicability.

Author Contributions: N.-V.F.: writing—review and editing, writing—original draft, visualization, validation, supervision, software, resources, project administration, methodology, investigation, formal analysis, data curation, conceptualization. G.C.: writing—review and editing, writing—original draft, resources, methodology, investigation, formal analysis, data curation, conceptualization and A.-A.D.: Writing—review and editing, writing—original draft, methodology, investigation, investigation, formal analysis. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and approved by the Ethics Committee of the Faculty of Economic Sciences of the Valahia University of Târgoviște no. 1487 of 30 August 2025.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data will be made available on request.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Items Excluded During Pilot Testing (EFA): Full Wording and Rationale

Selection criteria: retain items with loading ≥ 0.60 and no cross-loading > 0.40. Items not meeting these thresholds were excluded to improve construct validity and reliability before full data collection.

Construct	Item	Reason for Exclusion	Loading	Max Cross-Loading
Privacy (P)	"I want to have full control over whether my personal data is shared with third parties."	Cross-loading > 0.40	0.58	0.44
Ethics (E)	"Online platforms should practice transparent pricing, without hidden costs."	Loading < 0.60	0.59	0.33
Protection (Pr)	"I feel safer when e-commerce platforms provide detailed anti-fraud certifications."	Cross-loading > 0.40	0.62	0.41
Security (S)	"I trust the integrity of e-commerce servers to keep my data safe."	Wording ambiguity/ cross-loading	0.57	0.42
Trust (T)	"I feel more confident when the online merchant provides a visible physical address."	Loading < 0.60	0.56	0.35
Intention (IC)	–	–	–	–

Note: Excluded items were part of the initial survey instrument, but did not meet the psychometric thresholds during pilot testing. Their full wording is reported here for transparency. The exclusion reflects the cultural and contextual specificities of the Romanian respondents. For example, items referring to third-party data control or merchant addresses may have been perceived as 'granted' under GDPR compliance, reducing their variance. Similarly, "transparent pricing" and "anti-fraud certification" were interpreted as general expectations rather than distinct evaluative criteria. Although excluded, disclosing these items ensures replicability of the study and methodological transparency.

Table A1. Results of exploratory factor analysis (EFA).

Construct	KMO	Bartlett's Test χ^2 (df), p	No. of Factors Retained	Explained Variance (%)	Extraction Method	Rotation Method
Privacy (P)	0.764	$\chi^2 = 591.629$ (df = 6), $p < 0.001$	1	71.53%	PCA	Varimax
Ethics (E)	0.724	$\chi^2 = 400.347$ (df = 6), $p < 0.001$	1	59.40%	PCA	Varimax
Protection (Pr)	0.715	$\chi^2 = 320.957$ (df = 6), $p < 0.001$	1	60.42%	PCA	Varimax
Security (S)	0.772	$\chi^2 = 549.792$ (df = 6), $p < 0.001$	1	70.63%	PCA	Varimax
Trust (T)	0.741	$\chi^2 = 430.652$ (df = 6), $p < 0.001$	1	63.10%	PCA	Varimax
Total	0.696	–	5	77.03%	PCA	Varimax

Table A2. Rotated component matrix [a].

Item	Privacy (P)	Ethics (E)	Protection (Pr)	Security (S)	Trust (T)
Privacy (P)					
P1.1	0.846	–	–	–	–
P1.2	0.844	–	–	–	–
P1.3	0.668	–	–	–	–

Table A2. *Cont.*

Item	Privacy (P)	Ethics (E)	Protection (Pr)	Security (S)	Trust (T)
P1.4	0.492	–	–	–	–
Ethics (E)					
E2.1	–	0.766	–	–	–
E2.2	–	0.544	–	–	–
E2.3	–	0.633	–	–	–
E2.4	–	0.543	–	–	–
Protection (Pr)					
Pr3.1	–	–	0.598	–	–
Pr3.2	–	–	0.751	–	–
Pr3.3	–	–	0.679	–	–
Pr3.4	–	–	0.718	–	–
Security (S)					
S4.1	–	–	–	0.539	–
S4.2	–	–	–	0.823	–
S4.3	–	–	–	0.864	–
S4.4	–	–	–	0.639	–
Trust (T)					
T5.1	–	–	–	–	0.663
T5.2	–	–	–	–	0.689
T5.3	–	–	–	–	0.736
T5.4	–	–	–	–	0.624

Note: extraction method: principal component analysis; rotation method: varimax with Kaiser normalization; a. → rotation converged in nine iterations. Some pilot items exhibited loadings < 0.70 or cross-loadings > 0.40 and were therefore excluded before the final measurement model evaluation (see Table 5). Only retained items with loadings ≥ 0.70 were included in the confirmatory factor analysis and structural model estimation.

All measurement items used in this study were adapted from previously validated scales, as summarised in Table 4 (Section 3.5). The table below provides the exact wording presented in the survey, the original source scale, and a brief rationale confirming the alignment between each indicator and its definition of the construction. Minor wording adjustments were made during the translation and pretesting process, as described in Section 3.5.

Table A3. Provenance and alignment of measurement items.

Construct	Item Wording (Survey)	Source Scale	Rationale/Alignment
Privacy (P1.1)	"I am concerned about my online experience when personal data are requested."	CFIP, Smith, Milberg and Burke (1996) [120]	Captures concern with online privacy context, core to privacy definition.
Privacy (P1.2)	"I am concerned that my personal data may be reused for resale without my consent."	CFIP, Smith, Milberg and Burke (1996) [120]	Reflects risk of unauthorised reuse of data, central to privacy.
Privacy (P1.3)	"I want to control who has access to my personal data online."	CFIP, Smith, Milberg and Burke (1996) [120]	Captures access-control dimension of privacy.
Privacy (P1.4)	"I expect fair practices in the collection of my personal data."	CFIP, Smith, Milberg and Burke (1996) [120]	Aligns with fairness in data collection, part of privacy construct.
Ethics (E2.1)	"The information provided by this platform is of high quality."	Perceived Organizational Ethics Scale, Hunt, Wood and Chonko (1989) [121]	Captures ethical dimension of information quality.
Ethics (E2.2)	"The platform engages in mutual and transparent communication."	Hunt, Wood and Chonko (1989) [121]	Reflects reciprocity and fairness in communication.
Ethics (E2.3)	"The company respects ethical norms in its operations."	Hunt, Wood and Chonko (1989) [121]	Directly aligned with ethical compliance.

Table A3. *Cont.*

Construct	Item Wording (Survey)	Source Scale	Rationale/Alignment
Ethics (E2.4)	"The company provides fair and responsible assistance."	Hunt, Wood and Chonko (1989) [121]	Represents ethical responsibility toward consumers.
Protection (Pr3.1)	"The platform provides security certification for transactions."	IUIPC, Malhotra, Kim and Agarwal (2004) [122]	Institutional safeguard, consistent with protection definition.
Protection (Pr3.2)	"The availability of customer reviews and FAQ sections makes me feel protected."	IUIPC (adapted)	Consumer-facing cue interpreted as a perceived protection signal.
Protection (Pr3.3)	"The platform offers fraud certification."	IUIPC, Malhotra, Kim and Agarwal (2004) [122]	Reflects fraud-prevention safeguard.
Protection (Pr3.4)	"The platform guarantees return of goods, services, or money."	IUIPC, Malhotra, Kim and Agarwal (2004) [122]	Consumer rights protection, aligned with protection.
Security (S4.1)	"This platform ensures internet security."	Salisbury et al. (2001) [123]	General technical safeguard for security.
Security (S4.2)	"This platform ensures web security and integrity."	Salisbury et al. (2001) [123]	Captures website-level safeguards.
Security (S4.3)	"The platform ensures integrity of e-commerce personnel."	Salisbury et al. (2001) [123]	Human-resource safeguard dimension of security.
Security (S4.4)	"The platform ensures server integrity."	Salisbury et al. (2001) [123]	Technical infrastructure safeguard.
Trust (T5.1)	"I trust the platform for online payments."	Gefen, Karahanna and Straub (2003) [70]	Captures financial trust aspect.
Trust (T5.2)	"I trust the relationships and transactions on this platform."	Gefen, Karahanna and Straub (2003) [70]	Relational trust dimension.
Trust (T5.3)	"I trust the platform's technical infrastructure."	Gefen, Karahanna and Straub (2003) [70]	Structural assurance dimension of trust.
Trust (T5.4)	"I trust the information about products and services provided."	Gefen, Karahanna and Straub (2003) [70]	Cognitive trust in information quality.
Intention (I6.1)	"I will continue to use e-commerce."	UTAUT2, Venkatesh, Thong and Xu (2012) [124]	Reflects behavioural continuity.
Intention (I6.2)	"I will continue to visit e-commerce websites."	UTAUT2, Venkatesh, Thong and Xu (2012) [124]	Habitual component of intention.
Intention (I6.3)	"I enjoy shopping online."	UTAUT2, Venkatesh, Thong and Xu (2012) [124]	Affective component of intention.
Intention (I6.4)	"I recommend e-commerce to my friends."	UTAUT2, Venkatesh, Thong and Xu (2012) [124]	Word-of-mouth intention, aligned with behavioural intention.

Table A4. Structural model diagnostics (R^2, adjusted R^2, f^2, Q^2, PLSpredict).

Metric	Value	Interpretation
R^2 (Shopping Intention)	0.62	Substantial (>0.26, [151])
Adjusted R^2	0.61	—
f^2 Ethics	0.08	Small–Medium
f^2 Privacy	0.04	Small
f^2 Protection	0.18	Large
f^2 Security	0.12	Medium
f^2 Trust	0.06	Small
Q^2 (blindfolding)	0.41	>0 → predictive relevance
PLSpredict (RMSE, PLS vs. LM)	PLS < LM	Out-of-sample predictive power

Source: Authors' own work.

References

1. Alzahrani, A.M.; Alshamari, M.A. Comprehensive Assessment of Usable Security in E-Commerce Applications. *Int. J. Hum. Comput. Interact.* **2025**, 1–15. [CrossRef]
2. Frik, A.; Mittone, L. Factors Influencing the Perception of Website Privacy Trustworthiness and Users' Purchasing Intentions: The Behavioral Economics Perspective. *J. Theor. Appl. Electron. Commer. Res.* **2019**, *14*, 89–125. [CrossRef]
3. Gurung, A.; Raja, M.K. Online privacy and security concerns of consumers. *Inf. Comput. Secur.* **2016**, *24*, 348–371. [CrossRef]

4. Wang, C.L. Editorial–What is an interactive marketing perspective and what are emerging research areas? *J. Res. Interact. Mark.* **2024**, *18*, 161–165. [CrossRef]
5. Wang, C.L. Demonstrating contributions through storytelling. *J. Res. Interact. Mark.* **2025**, *19*, 1–4. [CrossRef]
6. Peltier, J.W.; Dahl Drury, A.J.; Khan, T. Cutting-edge research in social media and interactive marketing: A review and research agenda. *J. Res. Interact. Mark.* **2024**, *18*, 900–944. [CrossRef]
7. Wang, L.C. Interactive Marketing is the New Normal. In *The Palgrave Handbook of Interactive Marketing*; Springer-Nature International: Berlin/Heidelberg, Germany, 2023; pp. 1–12.
8. Chong, S.-E.; Ng, S.-I.; Bash, N.K.; Lim, X.-J. Social commerce in the social media age: Understanding how interactive commerce enhancements navigate app continuance intention. *J. Res. Interact. Mark.* **2024**, *18*, 865–899. [CrossRef]
9. Huang, Z.; Zhu, Y.; Hao, A.; Deng, J. How social presence influences consumer purchase intention in live video commerce: The mediating role of immersive experience and the moderating role of positive emotions. *J. Res. Interact. Mark.* **2023**, *17*, 493–509. [CrossRef]
10. Bandara, R. Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *Eur. J. Mark.* **2020**, *55*, 219–246. [CrossRef]
11. Bandara, R.; Fernando, M.; Akter, S. Addressing privacy predicaments in the digital marketplace: A power-relations perspective. *Int. J. Consum. Stud.* **2020**, *44*, 423–434. [CrossRef]
12. Liu, C.; Marchewka, J.T.; Ku, C.Y.-F. American and Taiwanese Perceptions Concerning Privacy, Trust, and Behavioral Intentions in Electronic Commerce. *J. Glob. Inf. Manag.* **2004**, *12*, 18–40. [CrossRef]
13. Breward, M. Perceived Privacy and Perceived Security and Their Effects on Trust, Risk, and User Intentions. In Proceedings of the Eighth World Congress on the Management of eBusiness (WCMeB 2007), Toronto, ON, Canada, 11–13 July 2007. [CrossRef]
14. Pathak, D.S.K.; Kumar, R. Exploring Consumer Perceptions in Online Shopping for Sustainable Economic Development. *Int. J. Multidiscip. Res.* **2024**, *6*, 1–15. [CrossRef]
15. Rizomyliotis, I. Consumer Trust and Online Purchase Intention for Sustainable Products. *Am. Behav. Sci.* **2024**. [CrossRef]
16. Tao, S.; Liu, Y.; Sun, C. Examining the inconsistent effect of privacy control on privacy concerns in e-commerce services: The moderating role of privacy experience and risk propensity. *Comput. Secur.* **2024**, *140*, 103794. [CrossRef]
17. Prastyanti, R.A.; Sharma, R. Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India. *J. Hum. Rights Cult. Leg. Syst.* **2024**, *4*, 354–390. [CrossRef]
18. Mustaffa, W.S.W.; Rahman, R.A.; Hudin, N.S.; Wahid, H.b.A.; Taib, R.M. The Effect of Trust on Behavioral Intentions: An Empirical Investigation among Malaysian Online Shoppers. *Int. J. Bus. Technol. Manag.* **2023**, *5*, 163–169. [CrossRef]
19. Lisdayanti, A.; Hapsari, A.Y. The influence of security perception and consumer trust on repurchase intention on e-commerce platforms. *Tech. Bus. Manag.* **2024**, *8*, 107–121. [CrossRef]
20. Khan, M.F. A study of consumer buying trust on e- commerce. *Indian Sci. J. Res. Eng. Manag.* **2024**, *8*, 1–5. [CrossRef]
21. Zaheer, M.A.; Anwar, T.M.; Iantovics, L.B.; Manzoor, M.; Raza, M.A.; Khan, Z. Decision-making model in digital commerce: Electronic trust-based purchasing intention through online food delivery applications (OFDAs). *J. Trade Sci.* **2024**, *12*, 220–242. [CrossRef]
22. Handoyo, S. Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon* **2024**, *10*, e29714. [CrossRef] [PubMed]
23. Rob, v.d.D. The trust factor in the digital economy: Why privacy and security is fundamental for successful ecosystems. In Proceedings of the International Telecommunications Society (ITS), Kyoto, Japan, 24–27 June 2017; Available online: https://hdl.handle.net/10419/168536 (accessed on 20 July 2025).
24. Fan, M.; Ammah, V.; Dakhan, S.A.; Liu, R.; Mingle, M.N.A.; Pu, Z. Critical Factors of Reacquainting Consumer Trust in E Commerce. *J. Asian Financ. Econ. Bus.* **2021**, *8*, 561–573. [CrossRef]
25. Gajendra, S.; Wang, L. Ethical perspectives on e-commerce: An empirical investigation. *Internet Res.* **2014**, *24*, 414–435. [CrossRef]
26. Shah, M.H.; Okeke, R.; Ahmed, R. Issues of Privacy and Trust in E-Commerce: Exploring Customers' Perspective. 2013. Available online: https://api.semanticscholar.org/CorpusID:168186289 (accessed on 18 July 2025).
27. Chellappa, R.K. Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security 1 Introduction. 2007. Available online: https://api.semanticscholar.org/CorpusID:2529115 (accessed on 20 July 2025).
28. Kim, D.J.; Ferrin, D.; Rao, H.R. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decis. Support Syst.* **2008**, *44*, 544–564. [CrossRef]
29. Gong, Z.; Jin, Y. The Influence of Perceived Privacy upon the Trust in E-commerce. In Proceedings of the 2008 International Seminar on Future Information Technology and Management Engineering, Leicestershire, UK, 20 November 2008; pp. 141–143. [CrossRef]
30. Martin, K.D.; Borah, A.; Palmatier, R.W. Data privacy: Effects on customer and firm performance. *J. Mark.* **2017**, *81*, 36–58. [CrossRef]

31. Riquelme, P.; Román, S. Is the influence of privacy and security on online trust the same for all type of consumers? *Electron. Mark.* **2014**, *24*, 135–149. [CrossRef]
32. Bélanger, F.; Crossler, R.E. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Q.* **2011**, *35*, 1017–1041. [CrossRef]
33. Otieno, E.A. Data protection and privacy in e-commerce environment: Systematic review. *GSC Adv. Res. Rev.* **2025**, *22*, 238–271. [CrossRef]
34. Yadav, D.; Kala, K.; Kolachina, R.I.R.; Kanneganti, M.C.; Pasupuleti, S.S. Data Privacy Concerns and their Impact on Consumer Trust in Digital Marketing. *Int. J. Sci. Res. Eng. Manag.* **2024**, *8*, 1–7. [CrossRef]
35. Jovanović, E.; Veinović, M.; Jovanović, M. Protecting User Data: Analysing Consent Notices and Behavioural Patterns in E-commerce. In Proceedings of the International Scientific Conference on Information Technology, Computer Science, and Data Science, Belgrade, Serbia, 8–11 September 2024; pp. 380–384. [CrossRef]
36. Blank, G.; Dutton, W. Age and Trust in the Internet: The Centrality of Experience and Attitudes Toward Technology in Britain. *Soc. Sci. Comput. Rev.* **2011**, *30*, 135–151. [CrossRef]
37. Zhang, R.; Li, Y.; Fang, L. PBTMS: A Blockchain-Based Privacy-Preserving System for Reliable and Efficient E-Commerce. *Electronics* **2025**, *14*, 1177. [CrossRef]
38. Patton, M.A.; Josang, A. Technologies for Trust in Electronic Commerce. *Electron. Commer. Res.* **2004**, *4*, 9–21. [CrossRef]
39. Smith, R.; Shao, J. Privacy and e-commerce: A consumer-centric perspective. *Electron. Commer. Res.* **2007**, *7*, 89–116. [CrossRef]
40. Bandara, R.; Fernando, M.; Akter, S. Privacy concerns in E-commerce: A taxonomy and a future research agenda. *Electron. Mark.* **2020**, *30*, 629–647. [CrossRef]
41. Yuniar, A.D. Thin privacy boundaries: Proximity and accessibility of E-commerce privacy policy in young consumers of Indonesia. *Int. J. Soc. Econ.* **2024**, *51*, 1182–1194. [CrossRef]
42. Zhuang, S. E-commerce consumer privacy protection and immersive business experience simulation based on intrusion detection algorithms. *Entertain. Comput.* **2024**, *51*, 100747. [CrossRef]
43. Castaldo, S.; Premazzi, K.; Zerbini, F. The Meaning(s) of Trust. A Content Analysis on the Diverse Conceptualizations of Trust in Scholarly Research on Business Relationships. *J. Bus. Ethics* **2010**, *96*, 657–668. [CrossRef]
44. Li, G.; Wu, H.; Wu, J.; Li, Z. Efficient and secure privacy protection scheme and consensus mechanism in MEC enabled e-commerce consortium blockchain. *J. Cloud Comput.* **2024**, *13*, 97. [CrossRef]
45. Chen, T.; Liu, F.; Shen, X.-L.; Wu, J.; Liu, L. Conceptualization of privacy concerns and their influence on consumers' resistance to AI-based recommender systems in e-commerce. *Ind. Manag. Data Syst.* **2025**, *125*, 1844–1868. [CrossRef]
46. Odoom, R.; Odoom, P.T.; Amu, P.Y.; Adams, M. Sustainable digital marketing practices and consumer brand engagement—A brand reputation mediation investigation. *J. Strateg. Mark.* **2025**, *33*, 254–270. [CrossRef]
47. Miklos, A.; Miklos-Thal, J. The ethics of online steering. *Ethics Inf. Technol.* **2024**, *26*, 43. [CrossRef]
48. Al Serhan, T.F.A.; Zhang, S. The paradox of digital marketing: Sustainable framework for effective strategies and regulatory challenges. *Inf. Dev.* **2025**, *41*, 529–545. [CrossRef]
49. Singh, C.; Dash, M.K.; Sahu, R.; Kumar, A. Investigating the acceptance intentions of online shopping assistants in E-commerce interactions: Mediating role of trust and effects of consumer demographics. *Heliyon* **2024**, *10*, e25031. [CrossRef] [PubMed]
50. Schlag, M.; Rocchi, M.; Turnbull, R. Adam Smith's Virtue of Prudence in E-Commerce: A Conceptual Framework for Users in the E-Commercial Society. *Bus. Soc.* **2024**, *63*, 1462–1502. [CrossRef]
51. Chorąś, M.; Pawlicka, A.; Jaroszewska-Chorąś, D.; Pawlicki, M. Not Only Security and Privacy: The Evolving Ethical and Legal Challenges of E-Commerce. In *Computer Security. ESORICS 2023 International Workshops*; Katsikas, S., Cuppens, F., Cuppens-Boulahia, N., Lambrinoudakis, C., Garcia-Alfaro, J., Navarro-Arribas, G., Nespoli, P., Kalloniatis, C., Mylopoulos, J., Antón, A., et al., Eds.; ESORICS 2023. Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2024; Volume 14398. [CrossRef]
52. Channak, Z.M.; Alkhateeb, A.; Saleh, E.; Aldeeb, H.; Alsharif, S. Business Ethics in E-Commerce—Legal Challenges and Opportunities. *Bus. Ethics E-Commer.* **2023**, *6*, 1–16. [CrossRef]
53. Pena-Garcia, N.; Horst, E. Loyalty beyond transactions: The role of perceived brand ethics in e-commerce. *Front. Commun.* **2025**, *10*, 1605171. [CrossRef]
54. Floridi, L. Information Quality. *Philos. Technol.* **2013**, *26*, 1–6. [CrossRef]
55. Mou, J.; Shin, D.; Cohen, J. Trust and risk in consumer acceptance of e-services. *Electron. Commer. Res.* **2017**, *17*, 255–288. [CrossRef]
56. Wiradendi, W.C.; Solikhah, S.; Fadillah, F.N.; Puji, L.D. Effectiveness of E-Training, E-Leadership, and Work Life Balance on Employee Performance during COVID-19. *J. Asian Financ. Econ. Bus.* **2020**, *7*, 443–450. [CrossRef]
57. Hipólito, F.; Dias, Á.; Pereira, L. Influence of Consumer Trust, Return Policy, and Risk Perception on Satisfaction with the Online Shopping Experience. *Systems* **2025**, *13*, 158. [CrossRef]
58. Farhat, R.; Yang, Q.; Ahmed, M.A.O.; Hasan, G. E-Commerce for a Sustainable Future: Integrating Trust, Product Quality Perception, and Online-Shopping Satisfaction. *Sustainability* **2025**, *17*, 1431. [CrossRef]

59. Aldera, S.; Alradhi, A.; Abanmi, N. Exploring the Impact of Consumer Trust on Purchase Intentions in Social Commerce: A Case Study of Saudi Arabia. *J. Inf. Syst. Eng. Manag.* **2025**, *10*, 154–168. [CrossRef]
60. Gao, Y.; Wu, X. A Cognitive Model Of Trust In E-Commerce: Evidence From A Field Study In China. *J. Appl. Bus. Res.* **2010**, *26*, 37–44. [CrossRef]
61. Solano, J.T.C.; Guzman, D.M.C.; Alvarez, J.C.E.; Costales, J.A.R. Ciberseguridad y protección de datos en e-commerce. *Univ. Soc.* **2025**, *17*, 108–118.
62. Yan, J. Data privacy regulation and cross-border e-commerce. *Empirica* **2024**, *51*, 913–927. [CrossRef]
63. Zhang, Y.; Zhang, T.; Yan, X. Understanding impulse buying in short video live E-commerce: The perspective of consumer vulnerability and product type. *J. Retail. Consum. Serv.* **2024**, *79*, 103853. [CrossRef]
64. Lia, Z.; Lee, G.; Raghu, T.S.; Shic, Z. Impact of the General Data Protection Regulation on the Global Mobile App Market: Digital Trade Implications of Data Protection and Privacy Regulations. *Inf. Syst. Res.* **2024**, *36*, 669–689. [CrossRef]
65. Raimi, L.S.; Abdullah, A.D.B.A.; Bamiro, N.B. Does the Digital Environment Impact E-Commerce Performance in Brunei Darussalam After the COVID-19 Pandemic? *J. Public Aff.* **2025**, *25*, e70020. [CrossRef]
66. Parisasadat, S.; Vlahu-Gjorgievska, E.; Yang-Wai, C. Enhancing privacy in mHealth Applications: A User-Centric model identifying key factors influencing Privacy-Related behaviours. *Int. J. Med. Inform.* **2025**, *199*, 105907. [CrossRef]
67. Truong Tuan, L.; Nguyen Thi Thanh, H. An extension of Trust and TAM model with TPB in the adoption of digital payment: An empirical study in Vietnam. *F1000Research* **2025**, *14*, 127. [CrossRef] [PubMed]
68. Liu, K.-J.; Chen, S.-L.; Huang, H.-C.; Gan, M.-L. The trust paradox: An exploration of consumer psychology and behavior in cross-border shopping using E-commerce mobile applications. *Acta Psychol.* **2025**, *254*, 104778. [CrossRef]
69. Roopnarain, M.; Mwapwele, S.D. Factors influencing the adoption and usage of blockchain in e-commerce: A systematic literature review. *Afr. J. Sci. Technol. Innov. Dev.* **2025**, *17*, 238–251. [CrossRef]
70. Gefen, D.; Karahanna, E.; Straub, D.W. Trust and TAM in online shopping: An integrated model. *MIS Q.* **2003**, *27*, 51–90. [CrossRef]
71. Yadav, P.; Keshri Keshri, K. Enhancing the Security of E-Commerce Systems Against Various Types of Attacks Using Deep Learning Model. *Int. J. Inf. Technol. Decis. Mak.* **2025**, *24*, 1801–1824. [CrossRef]
72. Kim, E.; Tadisina, S. A model of customers' trust in e-businesses: Micro-level inter-party trust formation. *J. Comput. Inf. Syst.* **2007**, *48*, 88–104. [CrossRef]
73. Palvia, P. The role of trust in e-commerce relational exchange: A unified model. *Inf. Manag.* **2009**, *46*, 213–220. [CrossRef]
74. Skitsko, V.; Ignatova, I. Modeling the process of purchase payment as a constituent of information security in e-commerce. *Oper. Res. Decis.* **2016**, *26*, 83–99. [CrossRef]
75. Ruppel, C.; Underwood-Queen, L.; Harrington, S.J. E-commerce: The roles of trust, security, and type of e-commerce involvement. *e-Serv. J.* **2003**, *2*, 25–45. [CrossRef]
76. Miyazaki, A.D.; Fernandez, A. Consumer perceptions of privacy and security risks for online shopping. *J. Consum. Aff.* **2001**, *35*, 27–44. [CrossRef]
77. Sun, Y.; Qu, Q. Platform Governance, Institutional Distance, and Seller Trust in Cross-Border E-Commerce. *Behav. Sci.* **2025**, *15*, 183. [CrossRef]
78. Qu, Y.; Baek, E. Let virtual creatures stay virtual: Tactics to increase trust in virtual influencers. *J. Res. Interact. Mark.* **2024**, *18*, 91–108. [CrossRef]
79. Kennedy, M.S.; Ferrel, L.K.; LeClair, D.T. Consumers' trust of salesperson and manufacturer: An empirical study. *J. Bus. Res.* **2001**, *51*, 73–86. [CrossRef]
80. Abyad, A. Importance of consumer trust in e-commerce, Business. *Middle East J. Bus.* **2017**, *12*, 20–24. [CrossRef]
81. Flavian, C.; Guinaliu, M. Consumer trust, perceived security privacy policy: Three elements of loyalty to a website. *Ind. Manag. Data Syst.* **2006**, *106*, 601–620. [CrossRef]
82. Habibi, R.; Hajati, Z. Trust in e-commerce. *Int. J. Innov. Appl. Stud.* **2015**, *10*, 917–922.
83. Papadoupoulou, P. Applying virtual reality for trust-building e-commerce environments. *Virtual Real.* **2007**, *11*, 107–127. [CrossRef]
84. Maamar, Z. Commerce, e-commerce, and m-commerce: What comes next? *Commun. ACM* **2003**, *46*, 251–257. [CrossRef]
85. Cheung, C.; Lee, M.K.O. Understanding consumer trust in internet shopping: A multidisciplinary approach. *J. Am. Soc. Inf. Sci. Technol.* **2006**, *57*, 479–492. [CrossRef]
86. Gefen, D.; Straub, D.W. Consumer trust in B2C e-commerce and the importance of social presence: Experiments in e-products and e-services. *Omega* **2004**, *32*, 407–424. [CrossRef]
87. Hampton-Sosa, W.; Koufaris, M. The effect of web site perceptions on initial trust in the owner company. *Int. J. Electron. Commer.* **2005**, *10*, 55–81. [CrossRef]
88. Park, J.; Shin, W.; Kim, B.; Kim, M. Spillover effects of data breach on consumer perceptions: Evidence from the E-commerce industry. *Internet Res.* **2024**, *35*, 1–24. [CrossRef]

89. Singh, V.; Vishvakarma, N.K.; Kumar, V. Unmasking user vulnerability: Investigating the barriers to overcoming dark patterns in e-commerce using TISM and MICMAC analysis. *J. Inf. Commun. Ethics Soc.* **2024**, *22*, 275–292. [CrossRef]
90. Chang, M.K.; Cheung, W.; Tang, M. Building trust online- interactions among trust building mechanisms. *Inf. Manag.* **2013**, *50*, 439–445. [CrossRef]
91. Teo, T.S.H.; Liu, J. Consumer trust in e-commerce in the United States, Singapore and China. *Omega Int. J. Manag. Sci.* **2007**, *35*, 22–38. [CrossRef]
92. Petrovic, O.; Ksela, M.; Fallenbock, M.; Kittl, C.; Urban, G.L.; Zobel, R. *Trust in the Network Economy*; Springer: Santa Clara, CA, USA, 2003.
93. Lu, Y.; Zhao, L.; Wang, B. From virtual community members to C2C e-commerce buyers: Trust in virtual communities and its effect on consumers' purchase intention. *Electron. Commer. Res. Appl.* **2010**, *9*, 346–360. [CrossRef]
94. Fang, Y.; Qureshi, I.; Sun, H.; McCole, P.; Ramsey, E.; Lim, K.H. Trust, satisfaction, and online repurchase intention: The moderating role of perceived effectiveness of e-commerce institutional mechanisms. *MIS Q.* **2014**, *38*, 407–427. [CrossRef]
95. Oliveira, T.; Alhinho, M.; Rita, P.; Dhillon, G. Modelling and testing consumer trust dimensions in e-commerce. *Comput. Hum. Behav.* **2017**, *71*, 153–164. [CrossRef]
96. Wang, C.; Zhang, M. Empirical study the influences of customer orientation, service quality on behavioral intention based on China's consumer-to-consumer e-commerce context. *J. Balk. Tribol. Assoc.* **2016**, *22*, 2176–2195.
97. Thekkat, A.K.; Anandkumar, V.; Valacherry, A.K. Leveraging Trust for Value Creation: Enhancing Willingness to Use in Luxury E-Commerce Websites with Website Reputation and Third-Party Assurance. *J. Creat. Value* **2025**, *11*, 73–86. [CrossRef]
98. Pavlou, A.P. Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model. *Int. J. Electron. Commer.* **2003**, *7*, 101–134. [CrossRef]
99. Suri, A.; Sharma, Y.; Jindal, L.; Sijariya, R. Blockchain for data protection and cyber fraud reduction: Systematic literature review and technology adoption dynamics among gen Y and Z. *Int. J. Qual. Reliab. Manag.* **2024**, *41*, 2181–2198. [CrossRef]
100. Falahat, M.; Lee, Y.-Y.; Foo, Y.-C.; Chia, C.-E. A model for consumer trust in e-commerce. *Asian Acad. Manag. J.* **2019**, *24*, 93–109. [CrossRef]
101. Koufaris, M.; Hampton-Sosa, W. The development of initial trust in an online company by new customers. *Inf. Manag.* **2004**, *41*, 377–397. [CrossRef]
102. Sultan, F.; Urban, G.; Shankar, V.; Bart, Y. Determinants and role of trust in e-business: A large scale empirical study. *SSRN Electron. J.* **2003**, 1–44. Available online: http://hdl.handle.net/1721.1/1826 (accessed on 20 July 2025).
103. Ngo, Q.V.; Yang, Z. Ethics of retailer and customer citizenship behaviour in e-commerce: The role of perceived reputation and identification. *Eur. J. Int. Manag.* **2023**, *21*, 165–183. [CrossRef]
104. Luo, X.; Li, H.; Zhang, J.; Shim, J.P. Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decis. Support Syst.* **2010**, *49*, 222–234. [CrossRef]
105. Beldad, A.; de Jong, M.; Steehouder, M. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Comput. Hum. Behav.* **2010**, *26*, 857–869. [CrossRef]
106. Hair, J.F.; Hult, G.T.; Ringle, C.; Sarstedt, M.M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*; Sage Publishing: Thousand Oaks, CA, USA, 2022.
107. Faul, F.; Erdfelder, E.; Buchner, A.; Lang, A.-G. Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behav. Res. Methods* **2009**, *41*, 1149–1160. [CrossRef] [PubMed]
108. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.-Y.; Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psychol.* **2003**, *88*, 879–903. [CrossRef]
109. Armstrong, J.S.; Overton, T.S. Estimating nonresponse bias in mail surveys. *J. Mark. Res.* **1977**, *14*, 396–402. [CrossRef]
110. Groves, R.M.; Peytcheva, E. The Impact of Nonresponse Rates on Nonresponse Bias: A Meta-Analysis. *Public Opin. Q.* **2008**, *72*, 167–189. [CrossRef]
111. Coon, J.J.; Carena, J.v.R.; Morton, L.W.; Miller, J.R. Evaluating Nonresponse Bias in Survey Research Conducted in the Rural Midwest. *Soc. Nat. Resour.* **2020**, *33*, 968–986. [CrossRef]
112. Beaton, D.E.; Bombardier, C.; Guillemin, F.; Ferraz, M.B. Guidelines for the process of cross-cultural adaptation of self-report measures. *Spine* **2000**, *25*, 3186–3191. [CrossRef]
113. Sousa, V.D.; Rojjanasrirat, W. Translation, adaptation and validation of instruments or scales for use in cross-cultural health care research: A clear and user-friendly guideline. *J. Eval. Clin. Pract.* **2011**, *17*, 268–274. [CrossRef]
114. Kock, N. Common method bias in PLS-SEM: A full collinearity assessment approach. *Int. J. E-Collab.* **2015**, *11*, 1–10. [CrossRef]
115. Hair, J.F.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M.; Danks, N.P.; Ray, S. Mirror, mirror on the wall: A comparative evaluation of composite-based structural equation modeling methods. *J. Acad. Mark. Sci.* **2017**, *45*, 616–632. [CrossRef]
116. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]

117. Gefen, D.; Straub, D.; Boudreau, M.-C. Structural Equation Modeling And Regression: Guidelines For Research Practice. *Commun. Assoc. Inf. Syst.* **2000**, *4*, 1–70. [CrossRef]
118. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [CrossRef]
119. Gefen, D.; Rigdon, E.; Straub, D. An update and extension to SEM guidelines for administrative and social science research. *MIS Q.* **2011**, *35*, III–XII. [CrossRef]
120. Smith, H.J.; Milberg, S.J.; Burke, S.J. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Q.* **1996**, *20*, 167–196. [CrossRef]
121. Hunt, S.D.; Wood, V.R.; Chonko, L.B. Corporate ethical values and organizational commitment in marketing. *J. Mark.* **1989**, *53*, 79–90. [CrossRef]
122. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Inf. Syst. Res.* **2004**, *15*, 336–355. [CrossRef]
123. Salisbury, W.D.; Pearson, R.A.; Pearson, A.W.; Miller, D.W. Perceived security and World Wide Web purchase intention. *Ind. Manag. Data Syst.* **2001**, *101*, 165–177. [CrossRef]
124. Venkatesh, V.; Thong, J.Y.L.; Xu, X. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Q.* **2012**, *36*, 157–178. [CrossRef]
125. Hair, J.F.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M.; Danks, N.P.; Ray, S. Evaluation of Reflective Measurement Models. In *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*; Springer International Publishing: Cham, Switherland, 2021; pp. 75–90. [CrossRef]
126. Guerrero Luzuriaga, A.d.C.; García Ancira, C. Evaluación de Confiabilidad y Validez del Cuestionario que Mide el Nivel de Satisfacción: Hacia un Modelo Predictivo Efectivo. *Cienc. Lat. Rev. Cient. Multidiscip.* **2024**, *8*, 9991–10009. [CrossRef]
127. Hajjar, S.E. Statistical Analysis: Internal-Consistency Reliability and Construct Validity. 2018. Available online: https://api.semanticscholar.org/CorpusID:212534910 (accessed on 20 July 2025).
128. Kimberlin, C.L.; Winterstein, A.G. Validity and reliability of measurement instruments used in research. *Am. J. Health-Syst. Pharm.* **2008**, *65*, 2276–2284. [CrossRef]
129. Caparó, E.V. Validación de cuestionarios. *Odontol. Act. Rev. Cient.* **2018**, *1*, 71–76. [CrossRef]
130. Souza, A.C.; Alexandre, N.M.C.; Guirardello, E.B. Psychometric properties in instruments evaluation of reliability and validity. *Epidemiol. Serv. Saude* **2017**, *26*, 649–659. [CrossRef]
131. Carmines, E.G.; Zeller, R.A. *Reliability and Validity Assessment*; SAGE Publications, Inc.: Southend Oaks, CA, USA, 1979. [CrossRef]
132. Hair, J.F.; Risher, J.J.; Sarstedt, M.; Ringle, C.M. When to use and how to report the results of PLS-SEM. *Eur. Bus. Rev.* **2019**, *31*, 2–24. [CrossRef]
133. Henseler, J.; Sarstedt, M. Goodness-of-fit indices for partial least squares path modeling. *Comput. Stat.* **2013**, *28*, 565–580. [CrossRef]
134. Hair, J.F.; Black, W.C.; Babin, B.J.; Anderson, R.E. *Multivariate Data Analysis*; Pearson Education Limited: London, UK, 2014.
135. Jang, H.; Lee, S. Applying Effective Sensory Marketing to Sustainable Coffee Shop Business Management. *Sustainability* **2019**, *11*, 6430. [CrossRef]
136. Nemțeanu, M.S.; Dinu, V.; Pop, R.A.; Dabija, D.C. Predicting Job Satisfaction and Work Engagement Behavior in the COVID-19 Pandemic: A Conservation of Resources Theory Approach. *EM Econ. Manag.* **2022**, *25*, 23–40. [CrossRef]
137. Becker, J.M.; Ringle, C.M.; Sarstedt, M.; Völckner, F. How collinearity affects mixture regression results. *Mark. Lett.* **2015**, *26*, 643–659. [CrossRef]
138. Sobaih, A.E.E.; Elshaer, I.A. Personal Traits and Digital Entrepreneurship: A Mediation Model Using SmartPLS Data Analysis. *Mathematics* **2022**, *10*, 3926. [CrossRef]
139. Hulland, J. Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. *Strateg. Manag. J.* **1999**, *20*, 195–204. [CrossRef]
140. Bagozzi, R.P.; Yi, Y. On the evaluation of structural equation models. *J. Acad. Mark. Sci.* **1988**, *16*, 74–94. [CrossRef]
141. Nunnally, J.C. *Psychometric Theory*; McGraw-Hill: New York, NY, USA, 1978.
142. Nunnally, J.C.; Bernstein, I.H. *Psychometric Theory*, 3rd ed.; McGraw-Hill: New York, NY, USA, 1994.
143. Fornell, C.; Larcker, D.F. Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *J. Mark. Res.* **1981**, *18*, 382–388. [CrossRef]
144. Chin, W.W. How to Write Up and Report PLS Analyses. In *Handbook of Partial Least Squares*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 655–690.
145. Höck, M.; Ringle, C.M. Local strategic networks in the software industry: An empirical analysis of the value continuum. *Int. J. Knowl. Manag. Stud.* **2010**, *4*, 132–151. [CrossRef]
146. Hair, J.F.; Ringle, C.M.; Sarstedt, M. PLS-SEM: Indeed a silver bullet. *J. Mark. Theory Pract.* **2011**, *19*, 139–151. [CrossRef]

147. Sarstedt, M.; Hair, J.F.; Cheah, J.H.; Becker, J.M.; Ringle, C.M. How to specify, estimate, and validate higher-order constructs in PLS-SEM. *Australas. Mark. J.* **2019**, *27*, 197–211. [CrossRef]
148. Henseler, J.; Ringle, C.M.; Sarstedt, M. Testing measurement invariance of composites using partial least squares. *Int. Mark. Rev.* **2016**, *33*, 405–431. [CrossRef]
149. Dash, G.; Paul, J. CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technol. Forecast. Soc. Chang.* **2021**, *173*, 121092. [CrossRef]
150. Supriyanto, S.; Munadi, S.; Daryono, R.W.; Tuah, Y.A.E.; Nurtanto, M.; Arifah, S. The Influence of Internship Experience and Work Motivation on Work Readiness in Vocational Students: PLS-SEM Analysis. *Indones. J. Learn. Adv. Educ.* **2023**, *5*, 32–44.
151. Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed.; Lawrence Erlbaum Associates: Mahwah, NJ, USA, 1988.
152. Shmueli, G.; Sarstedt, M.; Hair, J.F.; Cheah, J.-H.; Ting, H.; Vaithilingam, S.; Ringle, C.M. Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. *Eur. J. Mark.* **2019**, *53*, 2322–2347. [CrossRef]
153. Dinev, T.; Hart, P. An Extended Privacy Calculus Model for E-Commerce Transactions. *Inf. Syst. Res.* **2006**, *17*, 61–80. [CrossRef]
154. Maignan, I.; Ferrell, O.C.; Ferrell, L. A stakeholder model for implementing social responsibility in marketing. *Eur. J. Mark.* **2005**, *39*, 956–977. [CrossRef]
155. Rindfleisch, A.; Malter, A.J.; Ganesan, S.; Moorman, C. Cross-sectional versus longitudinal survey research: Concepts, findings, and guidelines. *J. Mark. Res.* **2008**, *45*, 261–279. [CrossRef]
156. Aguinis, H.; Bradley, K.J. Best practice recommendations for designing and implementing experimental vignette methodology studies. *Organ. Res. Methods* **2014**, *17*, 351–371. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.