

The Effect of Security and Privacy on Albanian Customer Loyalty

EZMOLDA BAROLLI¹, BRUNILDA DURAJ², KLEI XHYHERI³

¹Department of Statistics and Applied Informatics, FE

University of Tirana

Rruga Arben Broci 1 1001, Tiranë

ALBANIA

²Department of Finance, FE

University of Tirana

Rruga Arben Broci 1 1001, Tiranë

ALBANIA

³Monetary Operations Department

Bank of Albania

Sheshi Skënderbej, Nr. 1, Tiranë

ALBANIA

Abstract: - The recent technological advancements and digital transformation across industries have highlighted the significance of trust that businesses must establish with customers in an increasingly digital world. Every action we take online generates a massive quantity of data, which we can use to improve customer experience, evaluate their buying habits, offer suggestions, collect health information, and so on. This research is based on two concepts: privacy and security. The goal of this paper is to discover the factors impacting Albanian customer loyalty based on their impression of privacy and security. Research questions and hypotheses have been developed to address the purpose of this paper and investigate how digital consumers react to privacy and security issues related to loyalty. The data gathered from a survey involving 703 people were analyzed using factor analysis, analysis of the econometric model and correlation. The findings of this study are intended to contribute to the advancement of consumer perception of privacy and security in Albania, as well as their impact on consumer loyalty.

Key-Words: - Online shopping, customer loyalty, perceived security, privacy of data, Albania, Digital trust.

Received: June 21, 2025. Revised: October 11, 2025. Accepted: November 5, 2025. Published: May 8, 2026.

1 Introduction

As more people use the internet for entertainment or buying, they are becoming more cognizant of their right to privacy. Information security systems aim to put in place safeguards that protect people's privacy. Thus, Internet users are becoming more conscious of potential security and privacy threats. Furthermore, security or privacy flows may discourage them from using an electronic service from a supplier that does not match their needs or expectations. The optimum (lowest) pricing for online services is not always a key consideration for the recipients of these services. Digital consumers may examine numerous factors, such as overall service quality, security, privacy, and the benefits they would receive from using the service.

Several compelling reasons justify the investigation of Internet users' perceptions of

privacy and security. Technology strongly affects privacy since it facilitates the digitalization of information, allowing anyone to easily collect and search for information. Because digitized information is largely irreversible, any activity by people in the digital realm exists in perpetuity. Digital consumers' knowledge of the weak privacy protection and the danger of privacy violation has grown dramatically.

The paper's major goal is to discover the main factors impacting Albanian customer loyalty based on their impression of privacy and security. Privacy, security, and loyalty are complex and dynamic phenomena that necessitate current research and analysis into their interrelationships. The main purpose is to learn how consumers evaluate privacy and security issues and how this influences their behavior in an online context.

To address this goal and to study how digital consumers react to privacy and security in relation to loyalty, the guiding research question has been developed: How do customers respond to loyalty based on privacy and security concerns in online shopping?

Many elements of loyalty are shared by online services and internet users. This suggests that client loyalty can be influenced by security and privacy. Customers' perceived privacy and security features for online services and internet users have a significant and favorable impact on customer loyalty, according to the study's key hypothesis.

The study of such a phenomenon is expected to be of great interest, particularly in a developing post-communist country like Albania. By focusing on this context, the study contributes to the literature dominated by mature e-commerce markets and provides insights applicable to other emerging economies. This study aims to improve the advancement of consumer understanding of privacy and security in Albania, as well as their impact on consumer loyalty. Online companies should work harder to favorably affect consumers' perceptions of privacy and security. Most businesses rely on contract renewals, which are driven by brand loyalty, to stay in business. They have a new strategy for increasing customer loyalty: establishing a personal sense of trust in their consumer base.

The findings of this study can help the organization in managing loyalty. The organization can collect client information, integrate analytical models, spot patterns, and use data to generate promotions and offers, as well as convey accurate messages to them at the right time and place. Through this study, private and public enterprises can identify ways to respond to customer requests for the design of various IT applications to ensure the security and privacy of online services.

Consumers, on the other hand, are concerned when personal information is exploited or inadequately protected. Identity theft, financial fraud, and other financial problems can emerge from a lack of privacy and security. This study can help consumers understand what they should look out for while using Internet services.

2 Literature Review

According to the literature, many studies on consumers influencing online shopping have been undertaken in the past, and several factors have been identified. This session will first define the concept of online purchasing before delving into how

security and privacy affect online shopping. It then focuses on four key constructs that form the theoretical foundation of the research model: perceived risk, privacy, security, and customer loyalty.

2.1 Online shopping

Since the mid-1990s, internet shopping, also known as electronic commerce, has been acknowledged as an alternate method of selling and purchasing goods and services. Selling online can benefit businesses in a variety of ways, including lower advertising expenses, reduced human resources, inventory, and time, and enhanced service quality. Reference [1], on the other hand, defines the downsides of online shopping as a lack of personal service, the inability to examine or handle the goods once they are intangible, and distribution and exchange issues, with credit card provision as the key factor. When it comes to the kind of people who typically use online shopping on the internet, Reference [2] indicates that gender, age, income, occupation, and education are important aspects that influence the purchasing decisions of online shoppers. Women, for example, shop online more than men [3], while men are more likely to buy high-involvement goods. Older and higher-income groups purchase more, while concerns over product quality, shipping, and returns remain barriers, [4], [5]. Some consumers are willing to overcome their fears and anxieties to save time and compete on price in online shopping. There are numerous elements that might impact a customer's decision to use or not utilize online purchasing services; they are classified as internal and external factors and include the following: perceived risk, privacy, security, experience, service quality, and consumer loyalty.

2.2 Perceived Risk

Reference [6] defines risk as a consumer's conviction that they will experience harm while seeking to accomplish a predefined objective. Risk is divided into smaller components, such as privacy, system and credit card security, fraud, and product issues. Furthermore, Reference [7] shows how risk can influence consumers' inclinations to buy electronic goods and services online. According to statistics, 80% of Internet users are reluctant to engage in online shopping because they cannot personally evaluate the product; approximately 50% are also thought to be unaware of online purchases due to a desire to use services after making a purchase, transaction uncertainty, and privacy concerns.

Customers' perceived risk is one of the main worries they have when shopping online because of the security given by that website or application, [8]. In contrast, they define privacy risk as the unintended hacking of others' private information during an online transaction. Client personal information and bank credit cards are related to perceived risk, [9]. As a result, security risk is seen as a critical factor in the online shopping environment and is extremely high.

Compared to traditional shopping, online consumers perceive higher risks overall, and this has a stronger influence on their choices than perceived benefits, [10]. Researchers have identified two main types of risk: product or service risks (e.g., quality, financial loss, wasted time) and transaction risks (e.g., privacy, security, and repudiation), [11], [12], [13]. Both categories strongly affect how consumers evaluate and adopt online shopping, underscoring why risk management is a priority for businesses.

2.3 Privacy

There are several studies on privacy-related issues since the rise of digital technology and the growth of the Internet [14], where privacy is defined as the right of people, or institutions to control when, how, and to what extent personal information is communicated to others [15], or as consumers' readiness to reveal personal information over the Internet [16]. All definitions state that the decision to share personal information is entirely up to the individual. However, as mentioned further in [16], it is apparent that the privacy concerns expressed by individuals over their personal information have an impact across e-commerce market and to realize its full potential, these concerns must be addressed.

Privacy, on the other hand, can be described as the level of control a person has over the information submitted on an e-commerce site, [17]. Individuals must regularly update their information for the purchase and delivery to be done effectively. However, the issue of privacy is vital for everyone, and the information provided must be protected according to security guidelines.

Few individuals understand how personalized advertisements function and how customized promotional messages are conveyed, posing a higher risk to consumer privacy, [18]. Privacy concerns stem from the fact that businesses must collect a large amount of consumer data so that they can deliver personalized advertisements. Although consumers value personalization, it raises worries about their personal information being collected and tracked without their consent, [14].

Researchers have defined privacy as one of the most critical ethical, legal, social, and political issues of the digital era, [19]. They have established distinct degrees of anxiety that customers may experience online to better comprehend the growing importance of privacy issues. Reference [19] addresses the six dimensions of internet privacy, based on earlier research, with improved definitions and comprehension. These are collection, secondary use, mistakes, incorrect access, control, and awareness. Each of them alludes to a worry that a person may experience when engaged in online activities, including privacy concerns, [19].

Trust and privacy are tightly linked. Strong data security builds loyalty [20], while poor safeguards erode it. Some consumers even create "virtual identities" to shield themselves, which complicates how companies manage customer information, [21]. Others adopt behavioral strategies when they feel at risk, such as withholding or falsifying information, or taking private and public actions to push back against data misuse, [22]. These patterns show that protecting privacy is not only a technical issue but also a cornerstone of building trust and repeat engagement.

2.4 Security

Security is equally important, too. Beyond honesty and trust, online businesses must demonstrate technical capacity to protect consumer data, ensure delivery, and handle payments securely, [23]. As Reference [16] points out, the market for electronic commerce is influenced by people's security worries about their personal information, and for it to reach its full potential, these issues must be addressed.

Reference [24] lists five characteristics of electronic trade security: The first four requirements are integrity, contract or obligation recognition, identification, secrecy and privacy, and availability. The recorded data must be valuable, secure, and accessible to the relevant people when needed. Additionally, the data must ensure that the user can be identified when doing essential transactions.

Electronic signatures, e-cards, network security software, and other security measures have been mentioned. These alternatives, nonetheless, lack total reliability, which influences how buyers perceive those businesses. It is very important that every organization develop internal standards for implementing appropriate security measures, [20]. The security risk increases as the organization becomes more accessible to the world, as do concerns that the company will be more subject to attacks.

This, in turn, can have a detrimental impact on the corporate environment, and the organization may abandon the e-commerce adoption process too soon, [25]. Furthermore, perceived business risk is defined as anxiety regarding an organization's business security when employing e-commerce technologies.

For businesses, security risks can cut both ways: they may discourage adoption, but they also pressure firms to innovate. For consumers, however, the stakes are immediate, financial transaction safety and protection from data misuse are decisive in shaping trust and loyalty, [20], [25].

2.5 Customer loyalty

Loyalty is the result of the behavior that connects the constructs of trust, privacy, and security. The research on social media provides an integrated picture of the critical roles that privacy and trust concerns play in shaping consumer purchasing behaviour, [26]. Reference [27] investigates the relationship between three common trust factors (suppliers, the Internet, and third parties) and attitudes regarding online transactions. The study used privacy and security concerns as moderating variables and discovered that these associations differed depending on how concerned consumers were when purchasing online. According to the survey, the 'fear' of the Internet as a place to do business continues to impede its use for e-commerce, although the existence of credible organizations mitigates this danger. Trust in the seller is essential in the business-customer interaction for the consumer to accept the risks associated with the transaction. Online customer behaviour theory's theoretical ramifications are also examined.

Loyalty can be defined both in terms of attitude and behavior. Reference [28] classified consumer loyalty into four groups: lack of loyalty, loyalty, hidden loyalty, and false loyalty, based on two dimensions: relative attitude and recurring business.

Marketing scholars should incorporate this loyalty classification in their research due to its major influence and repercussions. This classification includes both the behavioural and attitude dimensions of loyalty, [29].

In increasingly competitive markets, professionals are pushed to cultivate true brand loyalists with high relative attitudes and repeat purchasing behaviour. Firms are concerned about customer loyalty as it reduces acquisition costs, encourages repeated purchases, and generates word-of-mouth advocacy, [30].

Brand loyalty strengthens these dynamics through awareness and memory, [31], [32]. Awareness helps consumers identify brands through names, logos, or symbols, while memory connects brands to prior use contexts and needs fulfilled. Importantly, brands act as risk reducers, helping consumers feel more secure in their choices by mitigating functional, financial, social, and psychological risks, [31].

3 Theoretical Framework

Figure 1 depicts a research model outlining the constructs and relationships investigated in this paper based on the preceding discussion and hypotheses. The model, as a descriptive framework, does not show each hypothesis with a particular link, but it provides a way to organize the major constructs of the research. At a high level, the perceived security features cluster comprises information concerning the security and processing of client information.

The perceived privacy category includes legal considerations that protect privacy and ambiguity when making online purchases on the Internet. In addition, demographic variables, such as the relative importance of privacy and security features, as well as their influence on customer loyalty, will be examined in our model.

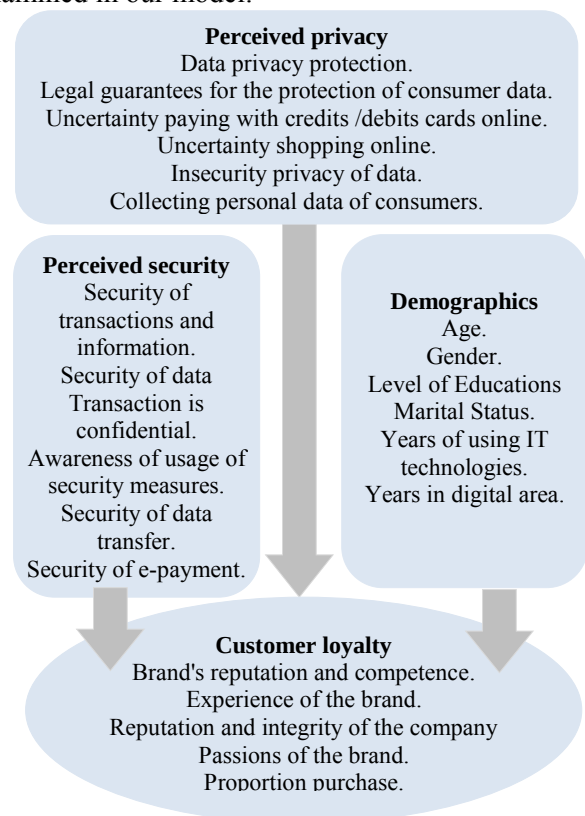


Fig. 1: Research model

Source: created by the authors

The question “How do customers respond to loyalty when they shop online based on privacy and security concerns?” aims to investigate the issues and difficulties experienced by businesses in Albania to further analyze and explore online shopping based on privacy and security.

The data gathered from this research will be used to gain a comprehensive understanding of these principles to solve problems in an appropriate way, allowing businesses to explore solutions with the primary goal of improving profits. The following are the objectives, research questions, and hypotheses.

Objective 1: Analysis of the frequencies of the factors considered during the study on the level of use of purchases online purchases, as well as some main concepts such as privacy and security.

This objective is achieved using descriptive analysis and, as such, does not support hypotheses but is based on factual findings from the analysis of responses received through questionnaires completed by customers of online businesses. More specifically, under this objective, it was aimed:

- 1.1 Identification of the average age of clients of online businesses.
- 1.2 Identification of educational level.
- 1.3 Assessment of the level of use of IT assets.
- 1.4 Assessment of the level of use of online shopping.
- 1.5 Identification of the average usage of IT technologies and the digital area.

Objective 2: Measure and describe the level of perceived security regarding personal data judgment when using online shopping.

Research questions guiding this objective are as follows:

- RQ 2.1: What is the nature of the relationship between online purchasing and perceived security?
 - H_0 : There is no significant relationship between online purchasing and perceived security.

- RQ 2.2: Which factor exerts the greatest influence on perceived security?

Objective 3: To examine the relationship of perceived privacy in online shopping.

Research questions guiding this objective are as follows:

- RQ 3.1: Which factor has the strongest influence on perceived privacy?
- RQ 3.2: What is the nature of the relationship between online purchasing and perceived privacy?

- H_0 : There is no significant relationship between online purchasing and perceived privacy.

4 Methodology

In defining the sample, literature offers a wide range of approaches, from studies with only a few participants to those with very large samples. A sample of 703 respondents is generally considered adequate to test relationships among variables in most types of research, [33]. According to this research, there are various characteristics that should be considered that are directly related to sample selection. These are the criteria:

- Attempting to be as representative as possible.
- To be chosen so that the mistake in the result is as small as feasible.
- Be appropriate for the sort of research.
- Be appropriate with respect to the analysis that will be performed.
- Its findings can be applied to other studies with the same level of certainty.

The factors that must be kept in mind regarding sample determination, on the other hand, correspond to some of its primary features, which include the population units that will engage in the research, the time span, the country, and the sample elements.

The technique utilized in this research is a non-probabilistic, intentional sample focused solely on the selection of individuals over the age of 18 to make the correct selection for gathering precise, full, and reliable information.

4.1 Survey Basis

The complexity of study design can be managed by developing a clear survey strategy that includes four stages: defining the goal, choosing the technique, planning, and implementation, [34]. The quality of the research is greatly affected by the appropriateness of the methodology, the research instrument, and the way the survey is conducted.

The sample size affects the accuracy of the results, so collecting more data would make the results more reliable and easily generalized. However, the sample size depends on the purpose of the study and the characteristics of the population. Reference [35] defines desired precision as the level of tolerable error in sample estimates. Factors that must be considered for determining the sample size include the purpose of the research, the size of the

population, sampling error, level of confidence, and the variance of the main variables, [36].

According to Reference [34], the decision to survey an entire population or to use a sample depends on feasibility and the acceptable level of error. Confidence levels are generally set at 95% or 99%, based on the Central Limit Theorem, which assures that the Mean of the sample approaches the population mean when sampling error is considered [37]. Considering the size of the sample required to achieve 99% accuracy of the collected and processed data, the authors decided against using probabilistic sampling and instead distributed the questionnaire using social media.

4.2 Research Instrument

In the drafting of the “Questionnaire to measure loyalty based on privacy and security concerns, several different authors were used, where the questions aim to explore how online shoppers react to privacy and security concerns in relation to loyalty.

The questionnaire consists of statements measured on a five-point Likert scale (1 = Not Important, 5 = Very Important). Items such as “Brand's reputation and competence when using online shopping” assess the role of brand trust in loyalty. In a dedicated section of the questionnaire with 10 questions, respondents were asked for demographic and IT-related information. It should be noted that the questions were mandatory, so the respondents needed to fill in information in all the sections of the questionnaire.

To analyze reliability and validity, factorial analysis was performed before Cronbach's alpha testing. Factor analysis helps reduce multiple observed variables into fewer latent dimensions, clarifying how the concepts are structured. The Kaiser-Meyer-Olkin (KMO) statistics and Bartlett's test of sphericity were used to assess sampling adequacy and correlation patterns. A KMO value close to 1 indicates compact correlations and supports the use of factor analysis, while values near 0 suggest weak factorability, [38]. Cronbach's alpha coefficients were then calculated to examine internal consistency, with values ≥ 0.70 considered acceptable for reliability, [39].

4.3 Testing Phase and Distribution

The authors piloted the questionnaire with 30 responders before constructing the online form for the complete population. The questionnaire initially featured several statements for each part; however, based on the results of the pilot survey, the authors discovered that respondents left the form unfinished

until the end. The preliminary survey also offered insight into the technique of data collecting, with many respondents claiming that online was the best and easiest approach for them.

The finalized questionnaire was hosted on Google Forms, allowing simple design, secure data collection, and easy access across devices. Before the release of the questionnaire, the configuration settings of the Google Form system allowed a person to respond only once, but still return to the questionnaire multiple times until the final submission. Anonymity was ensured, preventing any link between respondents and their data. The survey was distributed via social media across Albania's 12 prefectures to maximize coverage.

4.4 Data Analysis

Primary and secondary sources of information are used for research purposes. Secondary data used in the literature review were gathered from journals, manuals, theses, and books [40], while primary data were gathered through a structured questionnaire, a widely used survey tool that provides reliable quantitative data, [41].

The questionnaire's application will concentrate on the following sections: A - Demographics (age, gender, education, marital status, years using IT technologies, years in the digital area), B - Perceived Security (transaction security and confidentiality, security of data and information, security of e-payment, awareness of security measures), C - Perceived Privacy (privacy protection, legal guarantees, uncertainty in online payment, personal data concerns), and D - Customer Loyalty (brand reputation, experience of the brand, integrity of the company, proportion purchasing).

Cronbach's alpha, a measure of internal consistency, was employed in this study to examine the overall reliability of the measuring scale, where alpha gives an estimate of the percentage of total variation that is not due to error, which represents the scale's dependability, [42].

Data was coded and stored in a database, then analyzed using three approaches: descriptive analysis to profile respondents, factor analysis to validate constructs, and econometric modeling with correlation techniques to test relationships between security, privacy, risk, and loyalty.

4.5 Analyses of the Reliability of the Scales used in the Research Instruments

In the tables below are presented KMO and Bartlett values of factor analysis, which aim to measure the stability of each of the sections of the questionnaire.

Part of the survey was that 703 individuals completed the questionnaire, but for the factorial analysis for the modules, 343 individuals continued the questionnaire. Since the other people either have not made any online purchases or are not regular in these purchases, these are the people who will be analyzed further. For each of the module factors, the loadings range will be presented.

Factor analysis results for Module B (Table 1) demonstrate that perceived security regarding the personal data judgment when using online shopping went from 0.799 to 0.885 with a KMO value of 0.835, which is considered to be very good, meaning that it is appropriate to analyse the factors/variables in the study. This test showed that the variables for the perceived security regarding the personal data judgment when using online shopping had a significant correlation between them (highly significant Bartlett's test $p < 0.001$), indicating robust factorability (Table 1).

Table 1. Factorial analysis results for MODUL B:
Perceived security regarding the personal data
judgment when using online shopping

KMO value and Bartlett's Test

Kaiser-Meyer-Olkin value	.835
Chi-square value	890.021
Bartlett's Test of Sphericity	Degrees of freedom 6
Statistical significance	.000
Description of variables	Factor loadings
Security of transactions and information's	.827
Security of data	.845
The transaction is confidential	.850
Awareness of the usage of security measures	.885
Security of data transfer	.799
Security of e-payment	.805

Source: created by the authors

In Table 2 are presented KMO and Bartlett values, as well as factorial loadings of each statement, intending to measure the level of perceived privacy judgment when using online shopping (Module C). The factor loadings range is between 0.608 and 0.714 (Table 2). The KMO value for the scale for perceived privacy judgment when using online shopping is 0.693, which is considered to be very good, from which it can be concluded that it is appropriate to analyse the factors/variables in the study. Based on the significant Bartlett's results ($p < 0.001$), the test showed that the variables for this section had a significant correlation between

them, suggesting that the items reliably captured privacy concerns (Table 2).

Table 2. Factorial analysis results for MODUL C:
Perceived privacy judgment when using online
shopping

KMO value and Bartlett's Test

Kaiser-Meyer-Olkin value	.693
Chi-square value	782.283
Bartlett's Test of Sphericity	Degrees of freedom 6
Statistical significance	.000
Description of variables	Factor loadings
Data privacy protection	.621
Legal guarantees for the protection of consumer data	.608
Uncertainty paying with credit/debit cards online	.666
Uncertainty shopping online	.714
Insecurity privacy of data	.813
Collecting personal data of consumers	.736

Source: created by the authors

In Table 3 are presented the KMO and Bartlett values, as well as the factor loadings of each statement, which aim to measure the perceived customer loyalty when using online shopping (MODUL D). Factor loadings range from .580 to .798.

Table 3. Results of the factorial analysis for the
MODUL D: Perceived customer loyalty when using
online shopping

KMO value and Bartlett's Test

Kaiser-Meyer-Olkin value	.695
Chi-square value	1979.843
Bartlett's Test of Sphericity	Degrees of freedom 5
Statistical significance	.000
Description of variables	Factor loadings
Brand's reputation and competence when using online shopping	.730
Experience of the brand when using online shopping	.738
The reputation and integrity of the company where you buy online	.798
Passions of the brand	.580
Proportion purchase when using online shopping	.630

Source: created by the authors

The KMO value of 0.695 for perceived customer loyalty when using online shopping, which is considered to be very good, and a significant Bartlett's test ($p < 0.001$), confirm the appropriateness of the scale for analysis (Table 3).

The sections described above are analysed for the level of reliability and internal consistency using the Cronbach Alpha Coefficient. The following table shows the reliability coefficients based on the data of this study. As summarized in Table 4, the values of this coefficient range from zero to 1, where $r = 0.7$ or greater is considered sufficiently reliable [38]. The smallest value was recorded for the "Perceived privacy judgment when using online shopping" section ($\alpha = 0.693$), which is very close to the acceptable recommended level, while the highest was observed for "Perceived security regarding the personal data judgment when using online shopping" ($\alpha = 0.835$). These results confirm that the scales are reliable and internally consistent, providing a solid foundation for the following analysis.

Table 4. Reliability coefficients for the modules used

INSTRUMENTS	Number of variables (N)	Cronbach's alpha coefficient
MODUL B: Perceived security regarding personal data judgment when using online shopping	6	0.835
MODUL C: Perceived privacy judgment when using online shopping	6	0.693
MODUL D: Perceived customer loyalty when using online shopping	5	0.695
Total Study Questionnaire	17	0.741

Source: created by the authors

Taken together, the results confirm that privacy, security, and loyalty are measured consistently and validly, ensuring that the empirical analysis can directly test the relationships outlined in the research model (Figure 1).

4.6 Limitations of the Research

It is clear that every study also has some limitations. Even this study has its limitations as follows:

- The choice of the authors, filtering the sample of 703 respondents to 343 regular online shoppers, has improved the validity of the construct, but on the other hand, it has narrowed the scope by excluding fewer active consumers.

- Despite the relatively large sample size, the choice of a non-probabilistic method, a social media-based survey, can lead us to bias answers which could reduce the extent to which the findings can be generalized.
- While the study is related to measuring loyalty based on privacy and security concerns, the responses of individuals may not be so; they are a little subjective.
- The lack of comparison of the results of this study with other similar studies conducted in this field restricts the positioning of Albania's case within a broader international context.

Future research should employ probabilistic or mixed sampling methods, combine longitudinal or experimental designs, and explore computational modelling to strengthen representativeness and enhance comparative insights.

4.7 Ethical Considerations of the Research

Any study must protect the data collected about the people who answered the questionnaire. The legal framework for official statistics in Albania is defined by Law No. 17/2018 on Official Statistics [43]. According to this Law, the researchers must protect the data, and their processing must be done in such a way as not to violate the issue of confidentiality.

This means preventing the non-statistical use of the data obtained and the disclosure of the people who answered the questionnaire. The data used by the researchers cannot and should not be identified directly or indirectly.

5 Data Analysis and Results

5.1 Descriptive Statistics

The first goal of the research is to analyze the demographic profile of respondents and their engagement with online shopping, IT usage, and attitudes toward privacy and security. This goal is reached using descriptive analysis, which is not supported by hypotheses but is based on factual findings from the examination of questionnaire responses from all respondents.

About 703 individuals in Albania took part in the study, where 25.9% of them were men and 74.1% were women. Considering the aim of this study, we can reach the conclusion that online shopping is more preferred by women than men; this is a finding that is in line with the findings of Reference [3]. Figure 2 shows the gender distribution according to

age groups in the study. In the new age group of the study, the gender distribution is in favor of women, about 92.5.6% against men, 86.8%, while the age group over 59 is dominated by men, about 3.3%.

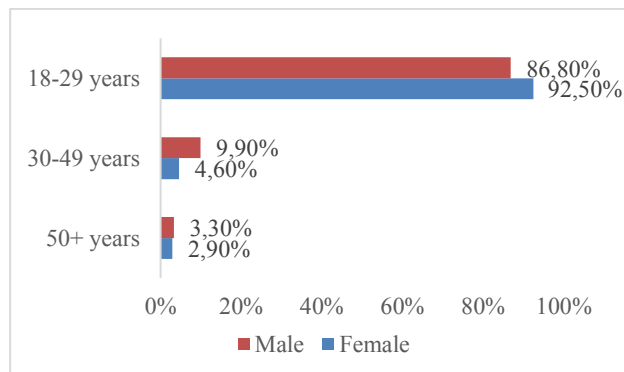


Fig. 2: Gender distribution by age group
Source: created by the authors

Regarding the age of the people who answered the questionnaire, their average age is 22.59 years, and there is a standard deviation of 6.54 years.

Individuals were also asked about the number of Years using IT technologies and the Number of Years using IT, internet, computers, Smartphones, etc. Thus, the minimum number of years using IT technologies is 1, and the maximum is 20 years, while the average number of years is 9.91 years, which has a standard deviation of 3.753 years. In relation to the Number of Years using IT, internet, computer Smartphone, the minimum is 1, and the maximum is 21 years, while the average is 10.74 years and has a standard deviation (SD) of 3.548 years. Table 5 presents descriptive statistics about the age of online clients regarding the two main variables: the number of years. Females have an average of around 10.4 years of using the internet and computer Smartphone while male 11.6 years.

Regarding the level of education, most of the people who participated in the study have a high level of education, where 81.7% have completed or are pursuing university studies, and 1.3% hold a PhD.

From the data in Figure 3, we underline that the participants in the study have a high level of education, and for this reason, we can say that they are a very good target group to give opinions about security, privacy, or online shopping.

Regarding the possession of IT equipment, Figure 4 presents the data for the people who answered our questionnaire. Almost all 98.01% have a smartphone, followed by computer owners 95.3%, and finally by tablet owners, around 34.57%.

Table 5. Descriptive statistics for online business clients

Demographic characteristics		Years of using IT technologies		Years of using IT internet, computers, and smartphones	
		Mean	SD	Mean	SD
Age Group	50+ years	15.5	2.1	17.6	2.6
	30-49 years	14.1	3.4	15.2	4.1
	18-29 years	9.4	3.5	10.2	3.0
Gender	Female	9.5	3.7	10.4	3.5
	Male	11.1	3.8	11.6	3.5
Level of Education	Basic 1 st and 2 nd Stage	13.5	1.6	13.5	1.6
	High School	9.0	3.3	9.0	3.0
	Voc. and Tech. School	8.0	2.8	12.0	3.3
	PhD	14.7	0.5	16.7	2.5
	University + Master	10.0	3.8	10.8	3.5
Married Status	Married	13.4	2.9	15.4	4.4
	Single	9.7	3.7	10.4	3.3

Source: created by the authors

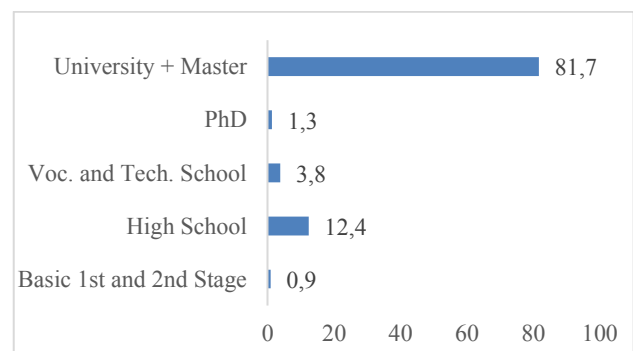


Fig. 3: Distribution of educational level
Source: created by the authors

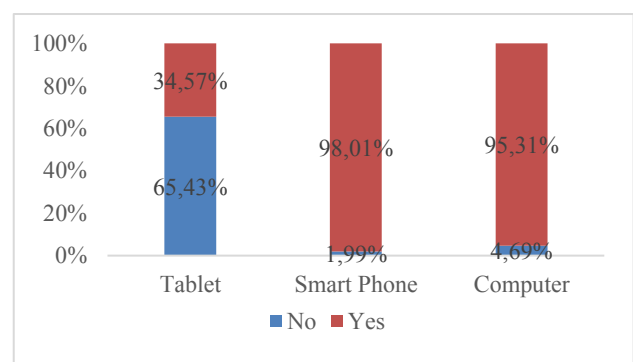


Fig. 4: Device ownership
Source: created by the authors

Regarding online shopping, 86.3% of participants had made at least one purchase, although only 56.5% considered themselves regular online buyers (Figure 5).

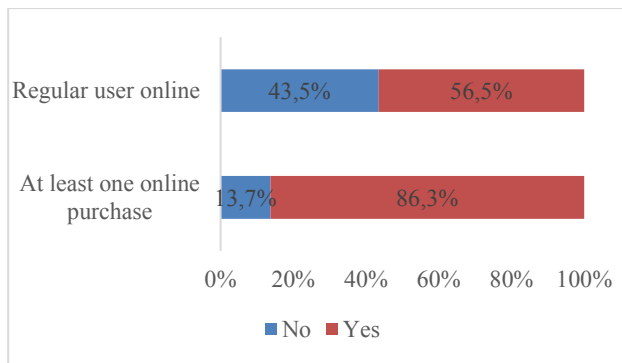


Fig. 5: Online shopping
Source: created by the authors

5.2 Security, Privacy, and Loyalty Scores

Descriptive statistics for the key constructs (Table 6) show that security concerns scored highest ($M = 4.17$, $SD = 0.93$), followed by privacy ($M = 4.02$, $SD = 0.99$) and loyalty ($M = 3.75$, $SD = 0.86$). These values indicate that, on average, consumers were strongly concerned about security and privacy, though somewhat less so about loyalty.

Table 6. Descriptive statistics for derived variables
Statistics

		Security	Privacy	Loyalty
N	Valid	343	343	343
Mean		4.1725	4.0190	3.7510
Std. Error of Mean		0.05003	0.05334	0.04642
Median		4.5000	4.3333	4.0000
Std. Deviation		0.92654	0.98793	0.85972
Minimum		2.00	2.00	2.00
Maximum		5.00	5.00	5.00

Source: created by the authors

Table 7 presents mean scores by demographic characteristics, revealing that younger and more digitally experienced respondents tend to report higher sensitivity to both security and privacy, which in turn affects their loyalty perceptions.

Figure 6, Figure 7 and Figure 8 illustrates the mean scores for the individual items within each construct. Respondents expressed the greatest concern for the security of electronic payments ($M = 4.22$) and transaction safety ($M = 4.20$) (Figure 6).

Table 7. Mean scores by demographic characteristics

Demographic characteristics		Security		Privacy		Loyalty	
		Mean	SD	Mean	SD	Mean	SD
Age Group	50+ y	4.17	0.11	4.33	0.26	4.00	0.72
	30-49 y	3.97	0.50	4.21	0.61	3.94	0.43
	18-29 y	4.20	0.98	3.99	1.03	3.72	0.91
	Total	4.17	0.93	4.02	0.99	3.75	0.86
Gender	Female	4.01	1.02	3.92	1.05	3.64	0.94
	Male	4.42	0.71	4.17	0.87	3.91	0.70
Level of Education	Basic	.	.	.	.	.	.
	High School	3.87	1.11	3.80	1.15	3.72	0.98
	Voc./Tech. School	4.92	0.09	4.58	0.26	4.00	0.21
	PHD	4.17	0.86	4.33	0.99	4.00	0.93
	University + Master	4.17	0.92	4.01	0.99	3.74	0.87
Married Status	Married	4.21	0.77	4.17	0.74	4.00	0.72
	Single	4.17	0.94	4.01	1.00	3.73	0.87
Tablet	No	4.34	0.96	4.08	1.06	3.71	0.95
	Yes	3.93	0.83	3.93	0.88	3.80	0.71
Smart Phone	No	4.33	0.43	5.00	0.61	4.00	0.50
	Yes	4.17	0.93	4.00	0.99	3.75	0.87

Source: created by the authors

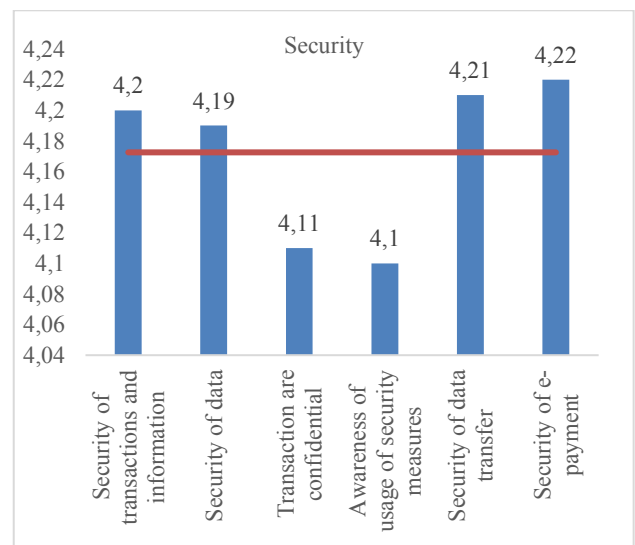


Fig. 6: Mean of Security
Source: created by the authors

For privacy, data protection ($M = 4.15$) and legal guarantees for consumer data ($M = 4.11$) were rated most highly (Figure 7).

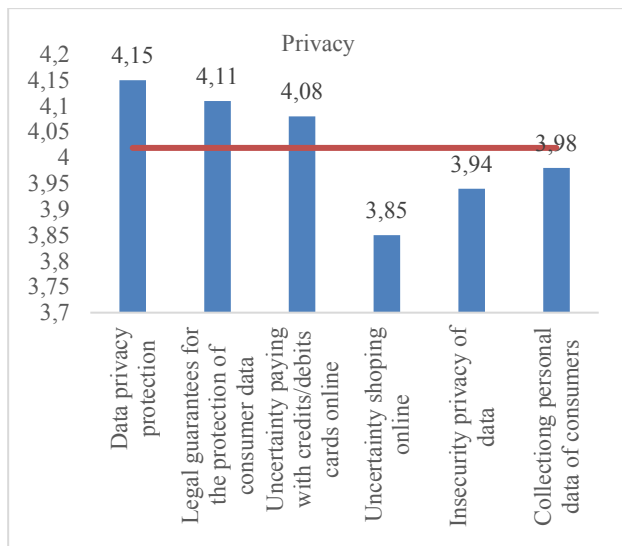


Fig. 7: Mean of Privacy
Source: created by the authors

Loyalty was most closely tied to company reputation and integrity (M = 4.00), followed by brand reputation and consumer experience (M = 3.81) (Figure 8).

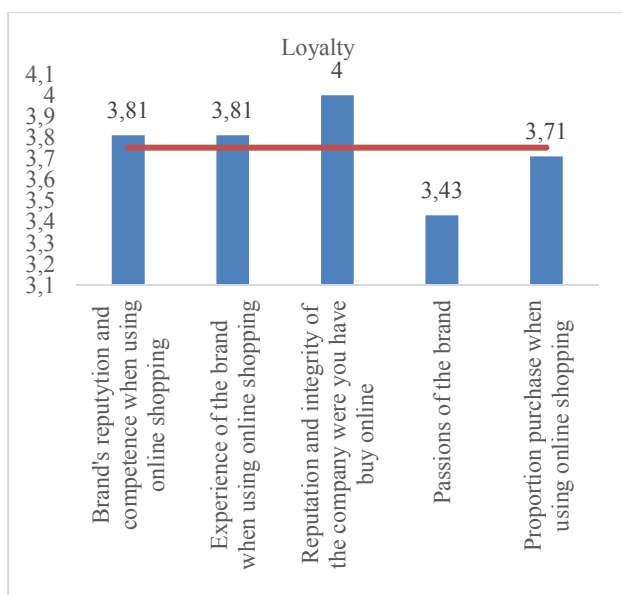


Fig. 8: Mean of Loyalty
Source: created by the authors

5.3 Correlation and Regression Analysis

To test the relationships between the constructs, Pearson's correlation coefficients were calculated (Table 8). Results revealed strong and significant positive correlations: security and loyalty ($r = 0.696$, $p < 0.01$), privacy and loyalty ($r = 0.690$, $p < 0.01$), and security and privacy ($r = 0.830$, $p < 0.01$). These results confirm that greater concern for security and privacy is strongly associated with greater customer loyalty.

Table 8. Pearson correlation matrix

Correlations

		Security	Privacy	Loyalty
Security	Pearson Correlation	1	.830**	.696**
	Sig. (2-tailed)		0,000	0,000
	N	343	343	343
Privacy	Pearson Correlation	.830**	1	.690**
	Sig. (2-tailed)	0,000		0,000
	N	343	343	343
Loyalty	Pearson Correlation	.696**	.690**	1
	Sig. (2-tailed)	0,000	0,000	
	N	343	343	343

** . Correlation is significant at the 0.01 level (2-tailed).

Source: created by the authors

To assess their relative importance, Ordinary Least Squares (OLS) regression was applied with security and privacy as predictors of loyalty (Equation 1). Table 9 reports the regression results, showing an R^2 of 0.525, meaning that over half of the variation in loyalty can be explained by these two constructs.

$$Loyalty = a_0 + a_1Security + a_2Privacy \quad (1)$$

Table 9. OLS results of the regression model

Model Summary

Model	R	R Square	Adjusted R-Square	Std. Error of the Estimate	Durbin-Watson
1	.724 ^a	0,525	0,522	0,59451	0,316

a. Predictors: (Constant), Privacy, Security

b. Dependent Variable: Loyalty

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	132,608	2	66,304	187,598	.000 ^b
	Residual	120,169	340	0,353		
	Total	252,777	342			

a. Dependent Variable: Loyalty

b. Predictors: (Constant), Privacy, Security

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0,955	0,149		6,391	0,000
	Security	0,367	0,062	0,395	5,893	0,000
	Privacy	0,315	0,058	0,362	5,387	0,000

a. Dependent Variable: Loyalty

Source: created by the authors

Security and privacy have a positive impact on digital consumer loyalty. Both predictors were statistically significant, with security ($\beta = 0.367$) exerting a slightly stronger effect than privacy ($\beta = 0.315$). The factor that Albanian consumers are most worried about when shopping online is the security of online shopping. The privacy part is important, but it is the second criterion when shopping online.

5.4 Summary of Findings

The findings identified in the previous sections validate the research model by confirming that perceived security and privacy have a significant impact on customer loyalty in online shopping. Security appears to be the leading concern, particularly electronic payment security, with an average score of 4.22, followed by transaction and information security with an average score of 4.2. Privacy remains closely related to security, but secondary factor, with an average of 4.15, followed by legal safeguards to protect consumer data with an average of 4.11. All these findings suggest that businesses seeking to build consumer trust in Albania's online market must prioritize secure payment systems, transparent data practices, and strong consumer protections.

Security and privacy have a positive impact on digital consumer loyalty. As a result, these findings are consistent with the overall conclusions reached from previous similar research available in the literature. While international research often emphasizes privacy as the dominant concern, Albanian customers are most worried about security when shopping online. This difference emphasizes the importance of contextualizing customers' behavior within the local digital market. In Section 6, we have compared these findings with international evidence to bring comparative cross-country insights.

6 Results and Comparative Discussion

The paper's major goal is to discover the main factors impacting Albanian customer loyalty based on their impression of privacy and security. From a statistical point of view, the findings show that there is an important and significant positive correlation ($r=0.830$, $p<0.01$) between security and privacy, indicating that among Albanian online shopping consumers, security and loyalty have a significant relationship. Security and privacy have a positive effect on online buyer regression, with security ($\beta = 0.367$) exerting a slightly stronger effect than privacy ($\beta = 0.315$). These findings show that both

dimensions are important, but payment and transaction security remain the main drivers of trust and loyalty among Albanian online customers. This fact shows that the digital market in Albania is still maturing, and concerns about the security of financial transactions influence consumer decisions.

To situate these findings in a broader perspective, Figure 9 summarizes indicators related to security, privacy and loyalty in different countries. Consumers in different countries differ in the weight they give to each dimension. This depends on culture, the maturity of online markets, and the protective measures applied by institutions.

For example, the literature shows that in Greece the importance given to privacy is influenced by cultural attitudes towards data sharing [2]; In the USA, studies show that increasing consumer trust depends heavily on transparent privacy policies and security certificates [8]; while for the loyalty of Generation Y consumers in Turkey, their security and experience are very important [20]. In China, privacy risks, particularly around data collection and unauthorized access, are predominant [19]. The above evidence and studies in different countries show the universal importance of security and privacy in building a loyalty relationship with consumers [27]. Put in this context, the Albanian online consumer appears to give more priority to security in e-payments in determining loyalty in the online market.



Fig. 9: Comparative cross-country insights on Privacy, Security, and Loyalty in online shopping
Source: assessment of authors based on [2], [8], [16], [19], [27]

Based on the above comparisons, Figure 10 reflects the relative weight of privacy and security in shaping loyalty across countries. The Albanian case demonstrates that security appears to be the leading concern compared to privacy in predicting loyalty. Here we have a difference with some other countries covered in this study, such as Greece or China, where privacy is valued almost equally with

security, or the USA, where strong privacy policies and security certificates determine consumer loyalty. This difference highlights that market maturity and trust in institutions influence the factors that consumers value most.

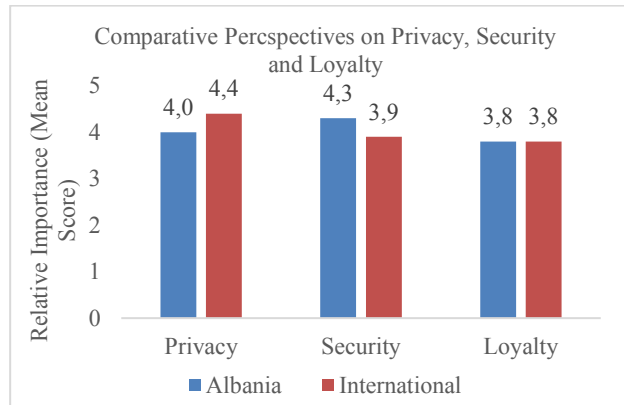


Fig. 10: Comparative strength of Privacy and Security as predictors of customer Loyalty across countries.

Source: assessment of authors based on [2], [8], [19], [20], [27], and this study

These results show that consumer behavior must be viewed in the cultural and developmental context of the country. The digital economy in Albania is still developing, and the main indicator to strengthen consumer loyalty seems to be the security of financial transactions. However, as the market matures, privacy concerns are likely to increase, following global trends. This means that businesses and policymakers must invest in payment system security, fraud prevention, and transparent practices to gain consumer trust. As the market matures and develops, it must pay close attention to privacy to ensure long-term consumer loyalty.

7 Summary and Conclusion

This study investigated the main factors impacting Albanian customer loyalty based on their impression of privacy and security. The study analyzed data collected from a questionnaire, which was distributed to 703 individuals, of whom 343 were active online shoppers. The data was analyzed using descriptive statistics, factor analysis, correlation, and regression modeling.

Results show that perceived security and privacy have a significant impact on customer loyalty in online shopping. Security appears to be the leading concern, particularly electronic payment security. These findings reinforce the need to build secure payment systems to create and maintain customer trust in emerging online markets.

The study extends the existing framework suggested in the researched literature, to an unexplored terrain such as Albania. Unlike other countries researched in the literature, in Albania, consumers prioritize security, especially e-payment security, which reflects the local level of digital maturity. This finding enriches the literature and emphasizes the need to design strategies adapted to the local context.

This study has several contributions: first, it provides one of the first large-scale quantitative analyses of the digital market in Albania; second, it identifies the importance of security over privacy in building customer loyalty in Albania; third it ensures validity through a focus on experienced online shoppers.

In conclusion, this study reinforces the importance of privacy and security in building customer loyalty and shows how the relative weight of these indicators varies from developed to developing countries. These findings have value for both academic and business.

References:

- [1] T. S. H. Teo, Attitudes Toward Online Shopping and the Internet, *Behaviour & Information Technology*, Vol. 21, No. 4, 2002, pp. 259-271. DOI: [10.1080/0144929021000018342](https://doi.org/10.1080/0144929021000018342)
- [2] L. Chai, P.A. Pavlou, From “Ancient” to “Modern”: A Cross-Cultural Investigation of Electronic Commerce Adoption in Greece and the United States, *The Journal of Enterprise Information Management* Vol. 17, No. 6, 2004, pp. 416-423. DOI: [10.1108/17410390410566706](https://doi.org/10.1108/17410390410566706)
- [3] D. Van den Poel, W. Buckinx, Predicting Online-Purchasing Behaviour, *European Journal of Operational Research*, Vol. 166, No. 2, 2005, pp. 557-575, ISSN 0377-2217, <https://doi.org/10.1016/j.ejor.2004.04.022>
- [4] X. Liu, and K. K. Wei, An Empirical Study of Product Differences in Consumers' E-commerce Adoption Behaviour, *Electronic Commerce Research and Applications*, Vol. 2, No. 3, 2003, pp. 229-239. DOI: [10.1016/S1567-4223\(03\)00027-9](https://doi.org/10.1016/S1567-4223(03)00027-9)
- [5] A. K. Kau, Y. E. Tang and S. Ghose, Typology of Online Shoppers, *Journal of Consumer Marketing*, Vol. 20, No. 2, 2003, pp. 139-156. DOI: [10.1108/07363760310464604](https://doi.org/10.1108/07363760310464604)
- [6] P. A. Pavlou, Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model,

International Journal of Electronic Commerce Vol. 7, No. 3, 2003, pp. 101-134.
<https://doi.org/10.1080/10864415.2003.11044275>

- [7] L. D. Zhou, and D. Zhang, Online Shopping Acceptance Model — a Critical Survey of Consumer Factors in Online Shopping, *Journal of Electronic Commerce Research*, Vol. 8, No. 1, 2007, pp. 41-62. (Accessed Date: Jan. 18, 2024)
- [8] Y. Bart, V. Shankar, F. Sultan, & G. L. Urban, Are the Drivers and Role of Online Trust Same for All Websites and Consumers? A Large-scale Exploratory Empirical Study, *Journal of Marketing*, Vol. 69, No. 4, 2005, pp. 133-152. DOI: [10.1509/jmkg.2005.69.4.133](https://doi.org/10.1509/jmkg.2005.69.4.133)
- [9] Y. Liebermann, & Sh. Stashevsky, Perceived Risks as Barriers to Internet and E-Commerce Usage, *Qualitative Market Research An International Journal*, Vol. 5, No. 4, 2002, pp. 291-300. DOI: [10.1108/13522750210443245](https://doi.org/10.1108/13522750210443245)
- [10] V-W. Mitchell, Consumer Perceived Risk: Conceptualizations and Models, *European Journal of Marketing*, Vol. 33, No. 1/2, 1999, pp. 163-195. DOI: [10.1108/03090569910249229](https://doi.org/10.1108/03090569910249229)
- [11] M. Featherman and P. Pavlou, Predicting E-Services Adoption: A Perceived Risk Facets Perspective, *International Journal of Human-Computer Studies*, Vol. 59, No. 4, 2003, pp. 451-474. [http://dx.doi.org/10.1016/S1071-5819\(03\)00111-3](http://dx.doi.org/10.1016/S1071-5819(03)00111-3)
- [12] A. H. Crespo, I. R. Del Bosque, and M. G. De los Salmones, The Influence of Perceived Risk on Internet Shopping Behaviour: A Multidimensional Perspective, *Journal of Risk Research*, Vol. 12, No. 2, 2009, pp. 259-277. DOI: [10.1080/13669870802497744](https://doi.org/10.1080/13669870802497744)
- [13] N. Li, P. Zhang, Consumer Online Shopping Attitudes and Behaviour: An Assessment of Research, *Eighth Americas Conference on Information Systems Proceedings*, 2002, pp. 508-517. (Accessed Date: Feb. 3, 2024).
- [14] C. Lee, D. A. Cranage, Personalisation–Privacy Paradox: The Effects of Personalisation and Privacy Assurance on Customer Responses to Travel Web Sites, *Tourism Management*, Vol 32, No. 5, 2011, pp. 987-994. DOI: [10.1016/j.tourman.2010.08.011](https://doi.org/10.1016/j.tourman.2010.08.011)
- [15] A. F. Westin, *Privacy and Freedom*, Scribner, 1967, ISBN 10: 0689102895, [ISBN 13: 9780689102899](https://doi.org/10.1016/j.tourman.2010.08.011). (Accessed Print Edition Date: Nov. 20, 2023).
- [16] F. Bélanger, J. S. Hiller, W. Smith, Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes, *Journal of Strategic Information Systems*, Vol. 11, No. 3-4, 2002, pp. 245-270. DOI: [10.1016/S0963-8687\(02\)00018-5](https://doi.org/10.1016/S0963-8687(02)00018-5)
- [17] G. Bansal & L. Chen. *If they trust our E-commerce Site, Will They Trust our Social Commerce Site Too? Differentiating the Trust in E-commerce and S-commerce: The Moderating Role of Privacy and Security Concerns*, Corpus ID: [6445165](https://doi.org/10.1016/S0963-8687(02)00018-5), 2011. (Accessed Date: Jan. 15, 2024).
- [18] C-D. Ham, Exploring How Consumers Cope with Online Behavioural Advertising, *International Journal of Advertising*, Vol. 36, No. 1, 2016, pp. 632-658. DOI: [10.1080/02650487.2016.1239878](https://doi.org/10.1080/02650487.2016.1239878)
- [19] W. Hong, J. Y. L. Thong, Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies, *MIS Quarterly*, Vol. 37, No. 1, 2013, pp. 275- 298. DOI: [10.25300/MISQ/2013/37.1.12](https://doi.org/10.25300/MISQ/2013/37.1.12)
- [20] A. Bilgihan, Gen Y Customer Loyalty in Online Shopping: An Integrated Model of Trust, User Experience and Branding. *Computers in Human Behaviour*, Vol. 61, No. 6, 2016, pp. 103-113. DOI: [10.1016/j.chb.2016.03.014](https://doi.org/10.1016/j.chb.2016.03.014)
- [21] N. M. A. Al-Slami, E-Commerce Security, *International Journal of Computer Science and Network Security*, Vol. 8, No. 5, 2008, pp. 340–354. [Link](#) (Accessed Date: Jan. 10, 2024).
- [22] J-Y. Son, S. S. Kim, Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model, *MIS Quarterly*, Vol. 32, No. 3, 2006, pp. 503-529. DOI: [10.2307/25148854](https://doi.org/10.2307/25148854)
- [23] B. Suh, I. Han, The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce, *International Journal of Electronic Commerce*, Vol. 7, No.3, 2003, pp. 135–161. <http://www.jstor.org/stable/27751068> (Accessed Date: Feb. 3, 2024).
- [24] K. C. Laudon, C. G. Traver, *E-Commerce: Business, Technology and Society*, Global Ed, Pearson Education Limited, 2023. [ISBN-10: 1292449721](https://doi.org/10.1016/j.tourman.2010.08.011). (Accessed Print Edition Date: Feb. 2, 2024).
- [25] K.-Y. Oh, A. R. Anderson, & D. Cruickshank, Perceived Barriers Towards the Use of e-Trade Processes by Korean SMEs, *Business Process Management Journal*, Vol. 18 No. 1, 2012, pp. 43-57. DOI: [10.1108/14637151211215000](https://doi.org/10.1108/14637151211215000)

- [26] M. Alzaidi, G. Agag, The Role of Trust and Privacy Concerns in Using Social Media for e-Retail Services: The Moderating Role of COVID-19, *Journal of Retailing and Consumer Services*, Vol. 68, No. 7, 2022, ISSN 0969-6989, DOI: [10.1016/j.jretconser.2022.103042](https://doi.org/10.1016/j.jretconser.2022.103042)
- [27] P. McCole, E. Ramsey, J. Williams, Trust Considerations on Attitudes Towards Online Purchasing: The Moderating Effect of Privacy and Security Concerns, *Journal of Business Research, Elsevier*, Vol. 63, No. 9-10, 2010, pp. 1018–1024. <https://doi.org/10.1016/j.jbusres.2009.02.025>
- [28] A. S. Dick, K. Basu, Customer Loyalty: Toward an Integrated Conceptual Framework, *Journal of the Academy of Marketing Science*, Vol. 22, No. 2, 1994, pp. 99-113. <https://link.springer.com/article/10.1177/0092070394222001> (Accessed Date: Feb. 17, 2024)
- [29] J. T. Bowen, S.-L. C. McCain, Transitioning Loyalty Programs: A Commentary on the Relationship Between Customer Loyalty and Customer Satisfaction, *International Journal of Contemporary Hospitality Management*, Vol. 27, No. 3, 2015, pp. 415-430. <https://doi.org/10.1108/IJCHM-07-2014-0368>
- [30] F. Ali, W. G. Kim, J. Li, H. M. Jeon, Make it Delightful: Customers' Experience, Satisfaction and Loyalty in Malaysian Theme Parks, *Journal of Destination Marketing & Management*, Vol. 7, 2018, pp. 1-11. <https://doi.org/10.1016/j.jdmm.2016.05.003>
- [31] K. L. Keller, V. Swaminathan, *Strategic Brand Management Building, Measuring, and Managing Brand Equity*, Pearson, ISBN 9781292314969, 2020. (Accessed Date: Oct. 3, 2024)
- [32] J.-N. Kapferer, *The new Strategic Brand Management: Advanced Insights and Strategic Thinking*, Kogan Page, ISBN-13 978-0749465155, 2012, [Online]. https://www.researchgate.net/publication/281803401_The_New_Strategic_Brand_Management (Accessed Date: Mar. 5, 2024).
- [33] J. P. Verma, P. Verma, *Determining Sample Size and Power in Research Studies: A Manual for Research*, Springer Nature Singapore, 2020. <https://doi.org/10.1007/978-981-15-5204-5>
- [34] L. Cohen, L. Manion, K. Morrison, *Research Methods in Education*, 8th ed. United Kingdom: Routledge /Taylor & Francis Group, ISBN 9781138209886, 2017. <https://doi.org/10.4324/9781315456539>
- [35] W. G. Cochran, *Sampling Techniques*, 3rd ed. New York: John Wiley & Sons, 1977. (Accessed Print Edition Date: Jan. 26, 2024).
- [36] R. Latpate, J. Kshirsagar, V. K. Gupta, G. Chandra, *Advance Sampling Methods*, Germany: Springer Nature Singapore, ISBN 978-981-16-0621-2, 2021, <https://doi.org/10.1007/978-981-16-0622-9>.
- [37] R. B. Dell, S. Holleran, & R. Ramakrishnan, Sample Size Determination, *ILAR Journal*, Vol. 43, No. 4, 2002. Pp. 207-213, <https://doi.org/10.1093/ilar.43.4.207>
- [38] N. K. Malhotra, *Marketing Research: An Applied Orientation*, 6th ed. United Kingdom: Pearson, ISBN 9781292265636, 2019. (Accessed Print Edition Date: Dec. 12, 2023).
- [39] A. Agresti, *An Introduction to Categorical Data Analysis*, 3rd ed. New York. NY: Wiley, ISBN 9781119405269, 2018. (Accessed Print Edition Date: Jun. 10, 2024).
- [40] J. E. Sallis, G. Gripsrud, U. H. Olsson, R. Silkos, *Research Methods and Data Analysis for Business Decisions: A Primer Using SPSS*, Switzerland: Springer International Publishing, 1st ed. ISBN: 978-3-030-84420-2, 2021. DOI: [10.1007/978-3-030-84421-9](https://doi.org/10.1007/978-3-030-84421-9)
- [41] E. Bell, B. Harley, A. Bryman, *Business Research Methods*. 6th ed., Oxford University Press, Oxford, ISBN: 9780198869443, 2022. (Accessed Print Edition Date: Mar. 10, 2024)
- [42] A. N. Oppenheim, *Questionnaire Design, Interviewing and Attitude Measurement*. Continuum, 2nd ed, ISBN-10: 0826451764, 2000. (Accessed Print Edition Date: Jan. 29, 2024)
- [43] INSTAT – Institute of Statistics, “Law No. 17/2018 on Official Statistics”, Republic of Albania, 2018, [Online]. <https://www.instat.gov.al/media/3972/law-no17-2018-on-official-statistics.pdf> (Accessed Dec. 21, 2024).

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Ezmolda Barolli was responsible for statistics, methodology development, data analysis, reviewing, and editing.

Brunilda Duraj and Klei Xhyheri conceived the presented idea, formulated the problem, carried out the literature review, and developed the theoretical framework.

The authors equally contributed to the presentation of the final findings of the research and comparative analyses.

Sources of Funding for Research Presented in a Scientific Article or the Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

https://creativecommons.org/licenses/by/4.0/deed.en_US