Science, Education and Innovations in the Context of Modern Problems
Issue 2, Vol. 9, 2026

RESEARCH ARTICLE

Data use ethics and its importance in gaining consumer trust: A study from a privacy perspective

Bessas Hocine
Doctor
Ferhat Abbas Sétif University 1
Algérie
Email: hocinebess@hotmail.com

Issue web link https://imcra-az.org/archive/392-science-education-and-innovations-in-the-context-of-modern-problems-issue-2-vol-9-2026.html

Keywords Data use ethics, consumer trust, and privacy protection.

Abstract

This study looks at data ethics and how it helps build consumer trust in Algerian digital platforms. Researchers used a descriptive-analytical method and a questionnaire in SPSS, with 190 young participants, The study tested three main ideas. First, it found a strong link between ethical data collection and how consumers view privacy protection. Second, it showed that being transparent about data use increases consumer trust, Third, it confirmed that privacy protection policies and technical security both help build consumer loyalty, The study suggests making privacy policies clear and easy to understand, investing in better encryption, and running awareness campaigns about data protection, It also recommends creating national data protection laws and making sure consumers give informed consent, The findings show that ethical data use is key to building trust and helping digital platforms succeed, which supports Algeria's growth in the digital sector.

Citation

Besas H. (2026). Data use ethics and its importance in gaining consumer trust: A study from a privacy perspective. *Science, Education and Innovations in the Context of Modern Problems*, 9(2), 1-14. https://doi.org/10.56334/sei/9.2.24

Received: 01.02.2025 | Accepted: 15.11.2025 | Published: 24.01.2026 (available online)

1. Introduction

With digital transformation, data has become the foundation of the knowledge economy and a crucial element in strategic decision-making within organizations. Intelligent data analysis has enabled companies to better understand consumer behavior and offer products that meet their needs and interests. Recent years have witnessed an increase in cases of privacy violations, leaks of sensitive data, and its exploitation for private purposes without the knowledge or consent of its owners. From this perspective, fundamental questions have arisen about how to balance the interests of companies in using data with the rights of individuals to protect their privacy and digital sovereignty. From a privacy perspective, this data reflects a person's identity and represents a part of their private life, making its protection a moral obligation before it is a legal one. Accordingly, data ethics has emerged as a multidisciplinary field that combines technology, law, philosophy, and sociology, with the aim of establishing a framework that regulates the relationship between institutions and consumers in the digital environment.

Ethics, at its core, is the compass guiding data use. Without ethical values, technology can transform from a means of improving lives into a tool for control, surveillance, and the violation of individual freedom. Therefore, respecting digital privacy has become an indicator of an organization's commitment to social responsibility and a prerequisite for building trust with customers. The modern consumer is more aware of the value of their personal information and more concerned with understanding how it is used, the purposes for which it is shared, and the measures taken

to protect it from breaches and leaks. Without this trust, the relationship between the organization and the consumer is at risk of disintegration, regardless of the quality of services or the distinction of the brand.

Hence the importance of this study, which seeks to analyze the relationship between data ethics and consumer trust, focusing on the ethical dimension of privacy as the foundation of digital trust. Building trust in the digital age requires a comprehensive vision that combines ethical commitment, legal compliance, and responsible innovation. Organizations that manage their customers' data transparently and respectfully enhance their reputation and earn their loyalty, while ignoring privacy leads to trust crises that are difficult to overcome. Data ethics is not merely a technical or legal issue; it is a human issue that affects the relationship between the individual and the digital society in an era where information has become a source of power.

This study's significance stems from its aim to analyze the relationship between data ethics and consumer trust, focusing on the ethical dimension of privacy as a foundation for digital trust.

1.1 Problem Statement

With the rapid development of digital technologies and the increasing reliance on data analytics in marketing decisions, data ethics has become a crucial factor in organizations' success in building long-term customer relationships. The unregulated use of personal information threatens individual privacy and weakens trust in organizations, while adherence to ethical principles in data collection and processing enhances credibility and increases customer loyalty. Despite regulatory and legislative efforts to protect privacy, the extent to which companies' commitment to data ethics impacts consumer trust, and how these practices influence consumer behavior and perceptions of digital organizations, remains a subject of debate. Therefore, this study focuses on analyzing the relationship between data ethics practices and consumer trust from a privacy perspective, by answering the following questions:

- To what extent does data collection ethics affect consumers' perception of the level of privacy protection?
- What is the impact of organizational transparency in data use on consumer trust in dealing with organizations?
- How do privacy protection policies contribute to enhancing consumer loyalty and brand trust?

1.2 Study Hypotheses

This study aims to examine how data use ethics affect consumer trust in organizations, focusing on the role of privacy as a mediating factor in building digital trust. Organizations that adhere to ethical principles in data collection, processing, and sharing are expected to achieve higher levels of acceptance and trust among their audiences compared to organizations that neglect these aspects. Based on this, the study hypotheses can be formulated as follows:

- There is a statistically significant relationship between data collection ethics and consumers' perception of the level of privacy protection.
- Organizational transparency in data use positively impacts consumer trust.
- There is a statistically significant relationship between the privacy protection policies implemented by organizations and the enhancement of consumer loyalty and brand trust.

1.3 Operational Definitions of the Study

- Data Use Ethics

Data use ethics refers to the principles that govern the collection, processing, storage, and sharing of personal data within organizations. These principles aim to ensure transparency, fairness, and respect for individual privacy, and to prevent harm or exploitation. In this study, we measure an organization's adherence to these principles through criteria such as informed consent, data minimization, and technical security, in addition to consumer surveys on the organization's practices. Ethics also encompasses adherence to ethical standards when using artificial intelligence and processing data to avoid bias and violations. These principles are essential for maintaining trust in the information society, especially with the accelerating pace of digitalization.

- Privacy (Information Privacy)

Information privacy refers to an individual's right to control their personal data in the digital environment, including protection from surveillance or unauthorized use. This also includes protecting personal data exchanged across digital platforms. In this study, this protection is measured by the consumer's awareness of the legal and technical means available to safeguard their data and prevent cybercrime. This requires a legal framework encompassing authorization, an administrative body for data protection, and judicial oversight of confidential communications.

Information privacy is linked to the challenges of the information society, where technology sometimes overrides ethical values, making the criminal protection of digital rights essential.

- Consumer Trust: Consumer trust is a feeling and behavior that emerges when a consumer perceives an organization as honest and transparent in handling their data. This leads to continued engagement and recommendation. This trust can be measured through indicators such as consumer satisfaction, repeat purchases, and loyalty resulting from ethical digital marketing. These indicators are assessed through surveys on the organization's image. Digital marketing enhances the organization's image by sharing values and benefits, reflecting consumer satisfaction and measuring purchasing behavior. A clear legal framework increases trust in digital platforms and helps build long-term relationships with consumers.

1.4 Previous Studies

1- A study by Dr. Attallah Lahcen, published in the Al-Muntada Journal for Economic Studies and Research in 2019, on the relationship between marketing ethics and customer loyalty for the Algerian electronics brand Condor. The research focused on the impact of practices such as transparency and social responsibility on customer loyalty, while also examining the role of satisfaction as a mediating factor. It sought to determine the strength of this impact using a statistical model and to assess its suitability for a local brand in a competitive market based on trust and quality.

The research used an online questionnaire to collect data, with a sample size of 115 participants. The study employed a quantitative, descriptive, and applied methodology, collecting data between December 2018 and June 2019. Data were analyzed using Structural Equation Modeling (SEM) via AMOS software to test the relationships between variables. The model relied on three main interrelated variables, excluding indicators with low loads. The results showed that marketing ethics has a strong and positive impact on satisfaction and loyalty, both directly and indirectly. The research recommended increasing social responsibility in marketing, such as transparent advertising and community support, to enhance satisfaction and loyalty. It also suggested conducting future studies with larger samples or additional variables, and replicating the study to monitor changes in consumer behavior. This research contributes to enriching the Arabic literature on marketing ethics and provides a practical guide for local brands. (Attallah, 2019)

2- Dr. Laboukh Hamid's study, "Ethical Artificial Intelligence and Data Privacy in Islamic Fintech," published in the Journal of Islamic Finance and Development Studies, Volume 6, Issue 11, 2025, discusses the ethical challenges that arise when using artificial intelligence in Islamic fintech. The study focuses on issues such as data privacy, consumer protection, and transparency. It analyzes these aspects by examining problems such as algorithmic bias, data leaks, and a lack of transparency in digital financial services. The study proposes solutions based on Islamic values such as justice and integrity to achieve a balance between innovation and ethical principles. It also aims to build a framework that combines innovation with Islamic values to create a fair and sustainable financial system, while enhancing trust in services through AI controls and emphasizing the importance of transparency.

The study employed a qualitative descriptive analytical approach, reviewing previous literature and studies without conducting field research or surveys. The results demonstrated the importance of establishing strict controls on artificial intelligence to ensure fairness and prevent bias, particularly in Islamic financial services that rely on profit and loss sharing. The results confirmed that transparency is essential for building trust between consumers and digital platforms. They also highlighted the need to integrate Islamic values such as honesty and equality into the development of technologies to achieve sustainable development and enhance trust in services such as digital payment and Islamic investment. The recommendations included developing Sharia-inspired Islamic regulatory frameworks for artificial intelligence, such as establishing joint religious and technological regulatory bodies to monitor algorithms, increasing awareness of data privacy, and encouraging future research on AI applications in Islamic finance with a focus on developing countries. It also recommended adopting adapted global standards to suit the Islamic context, which would help build an ethical and sustainable digital financial system that complies with Sharia principles and protects individual rights. Thus, the study contributes to bridging the gap between modern technology and Islamic heritage, and its findings are directed towards policymakers and practitioners in the field of Islamic financial technology. (Laboukh, 2025)

3- Dr. Gharib Al-Taous's study, entitled "Commitments to Digital Marketing Ethics and its Role in Consumer Protection," examined a sample of consumers and was published in the Journal of Finance and Markets, March 2022. The study aimed to assess the extent to which Algerian institutions adhere to digital marketing ethics and the impact of this on protecting digital consumer rights, such as the right to safety, access to accurate information, freedom of choice, and freedom of expression without misleading information. The research focused on measuring ethical commitment in online marketing, such as avoiding misleading advertisements and protecting data privacy, and examined the relationship between these ethics and consumer protection in Algeria. The study relied on a questionnaire as the primary data collection tool. The reliability of the questionnaire was confirmed using Cronbach's alpha coefficient. Ethical responsibility explained 13% of the variance in digital consumer protection in Algeria, with

significant differences based on gender and age. The study also highlighted the need to improve digital content to be more authentic and creative. (Taous, 2022)

2. Theoretical Framework of the Study

In today's digital economy, personal data has become one of the most important economic and strategic resources. It supports innovation in marketing, e-commerce, and artificial intelligence. With the increasing amount of digital data produced daily, it has become essential to understand personal data as facts related to consumer identity and to work on protecting it from violations. This section focuses on defining data and clarifying consumer rights related to it, relying on legal and ethical frameworks that balance the interests of companies with individuals' rights to privacy and control over their information.

2.1 The Concept of Data and Consumer Rights

Personal data is not merely a list of information, but rather any information that can identify an individual or influence their interactions within society (Solove, 2008). Therefore, a consumer's personal data includes information related to their legal identity, such as name, address, and telephone number, as well as financial and health data, which consumers generally prefer to keep confidential. In the realm of electronic payments and contracts, this data has become vulnerable to violation due to the ease with which it can be processed electronically. This necessitates legal protection to ensure its confidentiality and prevent its use or retention without consent (Basaid, 2022, p. 1395). Consumer data rights include the right to provide personal information only voluntarily, the right to receive complete and objective information about the product or service, the right to know the reasons for data processing, and the right to access, correct, or delete it. Electronic providers are obligated to maintain the confidentiality of this data. Algerian law requires data processors to adhere to the principles of legality and transparency and provides oversight mechanisms, such as the National Authority for the Protection of Personal Data, to impose penalties in cases of violations (Taous, 2022, p. 568)

In e-commerce, the consumer is often the weaker party because they are forced to provide sensitive data such as banking information, exposing them to the risks of fraud and identity theft. Therefore, the supplier must provide information protection that includes authorization, licensing, and secure processing, while guaranteeing the consumer's right to withdraw from the contract without additional costs. Studies indicate that consumer awareness helps them balance their needs and capabilities, enabling them to make informed decisions. (Ben Ali & Dah, 2020, p. 457)

The Algerian legal framework (such as Law 18-07) highlights the importance of data protection as a fundamental right linked to privacy, with proactive measures such as education and self-regulation to enhance trust in the digital market. This transforms the concept of data from mere technical information into a personal right that protects consumer dignity. (Ben Kara, 2019, p. 748)

2.2 Ethical Principles in Data Collection

With the digital transformation and the expansion of the data-driven economy, data collection has become an ethical responsibility, not just a technical procedure. Every decision regarding the type of data, how it is collected, who receives it, or how it is analyzed can have implications. This constitutes a violation of privacy or an injustice to certain groups. Therefore, ethical principles help achieve transparency and fairness, prevent exploitation and manipulation, and ensure that data remains a tool for improving understanding and decision-making, not a tool for harm or illegitimate control. (Shinar & Madasi, 2020, p. 264)

Basic Ethical Principles

1. Scientific Integrity and Honesty:

Floridi argues that honesty in data handling extends beyond technical protection to respect for human dignity. Personal information is an integral part of the "self," and any manipulation or dishonesty in managing this data constitutes an attack on personal identity, not merely a violation of privacy (Floridi, 2013, p. 244). The principle of scientific integrity and honesty is based on the honest collection, documentation, and analysis of data. This principle prohibits the fabrication, falsification, or deletion of information that does not align with the organization's expectations. It also requires the accurate documentation of data sources and collection circumstances. Furthermore, it encompasses respecting intellectual property and avoiding plagiarism. In the digital environment, integrity becomes even more crucial due to the ease with which figures can be inflated or unreliable data reused. Therefore, integrity is fundamental to public trust in research and the value of its results (Bouaam & Amri, 2020, p. 133).

2. The Principle of Data Quality:

The quality of personal data is a cornerstone in the era of the digital economy and artificial intelligence. Researchers recognize that personal data is not merely numbers, but strategic assets requiring precise and adequate standards. And relevant to the study's objective, because poor quality leads to misleading and biased results that may result in incorrect decisions regarding the individual (Redman, 2013). Ethically, collecting additional data that does not serve a clear purpose is prohibited because it increases the risk of privacy violations. This principle requires informing the participant about the type of data to be collected, the purposes of its use, the beneficiary, and the retention period. Furthermore, consent must be voluntary, explicit, and based on genuine understanding (Nour El-Din & Ben Adda, 2023, p. 60).

3. Do No Harm

The Do No Harm principle emphasizes the need to prevent any psychological, social, or economic harm that may result from data collection or use. This principle requires a prior risk assessment, such as the potential for stigmatization, blackmail, or unfair decisions based on the data. It also requires avoiding sensitive questions or unnecessary tracking procedures, providing the right to refuse to answer, and focusing on protecting vulnerable groups and preventing their exploitation or placing them at greater risk than others in digital applications. This principle includes preventing undisclosed secondary uses that may affect employment opportunities, services, or reputation. The goal here is protection. Human beings before protecting the results (Bouali and Obeidi, 2025, pp. 46-47). In addition to the above, researcher Helen Nissenbaum believes that harm to personal data does not only occur when data is stolen, but also when data is used outside the original context in which it was collected, such as using medical data for marketing purposes, for example, which is considered harm because it violates the context of the relationship between the patient and the doctor. (Nissenbaum, 2010)

4. The Principle of Fairness and Impartiality

This principle emphasizes that data collection and analysis must be fair and not lead to direct or indirect discrimination. For example, in the healthcare sector, a major study revealed that algorithms used in American hospitals to identify patients needing additional care were racially biased. This was because the algorithm relied on "previous healthcare costs" as personal data to predict healthcare needs. Since some patients had a history of being unable to pay, the system categorized them as needing less care compared to other patients with the same health condition (Obermeyer, Powers, Vogeli, and Mullainathan, 2019). Therefore, it is crucial to select a representative sample that prevents class, geographic, or cultural bias that could affect the results. Attention must also be paid to data and algorithm biases that may reflect historical injustices. Presenting results cautiously to avoid reinforcing stereotypes or producing knowledge used against specific groups contributes to fairness by making knowledge more equitable and realistic. (Ben Sghir, Al-Afri, & Hamel, 2021, pp. 138-139)

4.1 Consumer Trust and its Impact on Consumer Behavior

Consumer trust is a psychological and behavioral state that helps reduce the sense of risk in transactions and encourages purchasing decisions and interaction with institutions. This trust is linked to transparency and credibility in protecting personal data, which directly affects consumer loyalty and willingness to recommend the brand to others. Studies show a strong relationship between trust and consumer behavior, where consumers become more willing to take risks, such as sharing sensitive data, when the brand is known for its reputation and good performance. This increases the effectiveness of marketing campaigns. This trust is measured through indicators such as the level of overall satisfaction, the intention to purchase repeatedly, the willingness to pay a higher price, and the positive impact on the institution's image in the minds of customers, relying on metrics such as the SERVQUAL model adapted for the digital context. (Boudawd, 2013, p. 104) When consumer trust is high, they feel less threatened by privacy breaches or data misuse. This encourages them to share more personal information and engage in frequent online transactions without hesitation, especially in e-commerce, where consumers prefer platforms with a good reputation for data handling. In the Arab context, trust is linked to Islamic values such as wisdom, moderation, and justice. Ethical standards help achieve a balance between material needs and psychological values, increasing consumer loyalty to brands that respect these principles. Furthermore, trust-driven digital marketing leads to a positive customer response and increases the value of loyal customers by raising retention rates and recurring revenue, positively impacting the organization's economic performance.

When trust is high, consumer behavior shifts from negative to positive. Consumers become active advocates for the brand, recommending it through social media and personal networks. The negative impact of unethical or questionable promotional campaigns is also reduced because consumers filter out doubts themselves. Conversely, a loss of trust leads to avoidance of digital platforms, posting negative complaints online, and a rapid shift to competitors, increasing the cost of regaining lost customers compared to retaining existing ones. (Boudawd, 2013, p. 107)

5. Field Research Procedures

5.1 Study Methodology

This research employs a descriptive-analytical approach. The descriptive section focuses on the theoretical framework by reviewing scientific literature and previous studies on data ethics and consumer trust, aiming to construct a theoretical framework that supports the hypotheses.

The analytical part relies on a questionnaire administered to a sample of digital consumers in Algeria. Using a five-point Likert scale to measure ethical principles, trust, and privacy, the data is analyzed using SPSS software. This analysis employs descriptive statistics (means and standard deviations), Pearsonian correlation testing to measure the relationship between variables, and multiple linear regression analysis to identify causal effects. This process helps in proving hypotheses and drawing practical recommendations.

5.2 Research Limitations

Human Limitation: The research focuses on Algerian Generation Z consumers (18-27 years old) who use digital means in e-commerce. Therefore, the results cannot be generalized to other age groups, non-digital consumers, or areas with limited internet access.

Time Limitation: The research covers only the year 2026. Therefore, it does not address future changes in behaviors or new digital legislation.

Thematic Limitation: The research focuses solely on the ethics of using personal data in e-commerce and does not include other sectors such as banking or e-health. 3.3 Research Population and Sample

Due to the large size of the study population, which includes all users of e-commerce, and the lack of a sampling framework, relying on the random sampling method is not applicable. Therefore, the non-random sampling method was adopted, relying on a convenience sample of 190 individuals from Generation Z consumers in Algeria (18-27 years old), who were randomly selected according to their accessibility.

- Questionnaire

The study adopted the questionnaire as the primary tool for collecting quantitative data from the sample, given its ability to measure trends and opinions systematically and reliably. The questionnaire was designed based on the study's theoretical framework and research questions. It contributes to measuring the ethics of data use and its importance in gaining consumer trust. The questionnaire was divided into two sections:

Section One: This section includes psychometric data for the research sample related to gender, age, internet usage level, and the extent of internet use for purchasing.

Section Two: This section was divided into four axes as follows:

- Axis One: Data Collection Ethics (7 statements)

- Axis Two: Privacy Protection (7 statements)

- Axis Three: Institutional Transparency in Data Use (7 statements)

- Axis Four: Consumer Trust (7 statements)

- Verification of the questionnaire's validity and reliability through Cronbach's alpha test.

Table No. (01) Validity and Reliability Test using Cronbach's alpha coefficient

Statement	*Cronbach's alpha coefficient*	*Number of statements*
Data collection ethics	0.732	7
Privacy protection	0.751	7
Organizational transparency in data use	0.719	7
Consumer trust	0.768	7
Total survey	**0.843**	**28**

Source: SPSS v26 output

Cronbach's alpha test results showed that the questionnaire possesses a high degree of reliability and excellent validity, with an overall reliability coefficient of 0.843, which is higher than the minimum acceptable value (0.7). This indicates strong internal consistency across all 28 items. At the ax level, Cronbach's coefficients ranged from 0.719 to 0.768, all within the good to excellent range (>0.7), with the highest reliability observed in the consumer confidence axis (0.768) and the privacy protection axis (0.751). These results confirm the questionnaire's suitability for measuring the four variables with scientific accuracy. They also justify the use of the questionnaire in advanced statistical analyses such as correlation and regression with 95% confidence, and enhance the generalizability of the results to the digital Generation Z community in Algeria.

Analysis of the Psychometric Characteristics of the Study Sample

Table No. (02) Psychometric Data of the Study Sample

%	repetition	*Statement*	
55.3%	105	Male	Gender
44.7%	85	Female	
43.2%	82	18-21 years	Age
38.9%	74	22-24 years	
17.9%	34	25-27 years	
2.6%	5	Less than 2 hours	Internet usage level
13.2%	25	2 to 4 hours	
32.6%	62	4 to 6 hours	
51.6%	98	More than 6 hours	
78.9%	150	Yes	Academic specialization
21.1%	40	No	
100%	**190**	Total	

Source: SPSS v26 output

Psychometric analysis shows that the sample is scientifically suitable for studying data ethics and digital trust. The male majority (55.3%) indicates their greater activity in the digital sphere and their preference for online shopping. The 18-21 age group (43.2%) represents the most reliant on online platforms. Furthermore, 51.6% of participants use the internet for more than 6 hours daily, reflecting their suitability as a study population. The presence of 78.9% professionals reinforces their deep understanding of privacy concepts. Additionally, the balanced geographical distribution, including major cities, supports the representativeness and generalizability of the results to the local community.

Statistical Description of Study Variables

Table No. (03) Analysis of Agreement on Data Collection Ethics Axes

Ranking	*Relative Importance*	*Standard Deviation*	*Arithmetic Mean*	*Statement*	
2	0,74	0,99	3,70	The organization has the right to inform me of the type of data that will be collected before use begins.	1
1	0,75	1,06	3,76	I believe that data collection should be linked to a clear and beneficial goal for the consumer, and not just a commercial goal.	2

5	0,69	0,98	3,44	I believe that obtaining my explicit consent before collecting data is a fundamental ethical obligation for organizations.	3
3	0,72	1,04	3,61	I object to platforms collecting my data from other parties (such as social networks) without my knowledge.	4
4	0,72	1,07	3,61	I believe it is unethical to collect detailed data about my online behavior without informing me.	5
7	0,67	1,04	3,33	I believe I should have the ability to reject certain types of data without being completely deprived of the service.	6
6	0,69	0,98	3,43	In my opinion, respecting data collection ethics increases my trust in the organization and makes me more willing to deal with it.	7
	0.71	**0.03**	**3.55**	**the total**	

Source: SPSS v26 output

Table (3) shows that the sample members expressed moderate to high agreement with the principles of data collection ethics, with an overall mean of 3.55 out of 5. The second statement, "Data collection is linked to a clear and beneficial purpose for the consumer," ranked first (3.76, 75%), indicating high ethical expectations of applying the principle of benevolence and mutual benefit rather than mere commercial exploitation. The sixth statement, "The ability to refuse some data," ranked last (3.33, 67%) due to participants' fear of losing service, despite acknowledging their right to partial refusal. The systematic standard deviation (0.98-1.07) indicates a homogeneity of opinions and a strong collective agreement on the core ethical principles, reinforcing the relationship between ethical commitment and consumer trust in the digital environment.

Table (4) Analysis of the Extent of Agreement Regarding Privacy Protection Aspects

Ranking	*Relative Importance*	*Standard Deviation*	*Arithmetic Mean*	*Statement*	
7	0,71	1,02	3,56	I feel safe when the platform makes it clear that my data is stored in an encrypted and secure manner.	1
6	0,73	1,01	3,67	I prioritize using platforms that offer clear policies for data protection and privacy.	2
3	0,80	0,85	3,98	I am worried about the possibility of my personal data being leaked or my digital accounts being hacked.	3
5	0,76	0,90	3,80	I prefer to deal with platforms that allow me to permanently delete my account and all my data whenever I want.	4
1	0,82	0,69	4,12	I believe that organizations should invest in robust information security systems to protect consumer data.	5
2	0,80	0,68	4,02	I feel uncomfortable when I receive messages or advertisements from parties with whom I have not shared my data directly.	6
4	0,78	0,75	3,88	If a platform I use is subject to a security breach, it negatively affects my willingness to continue using it.	7
	0.77	**0.14**	**3.86**	**the total**	

Source: SPSS v26 output

Table (4) shows that the sample group highly agrees with the principles of privacy protection, with an overall average of 3.86 out of 5. Statement number 5, "Organizations invest in robust security systems," ranked first (4.12, 82%),

indicating high expectations of clear technical responsibility. This was followed by statement number 6, "Discomfort with unwanted advertising" (4.02, 80%), confirming their sensitivity to covert tracking. Statement number 1, "Feeling secure with encryption," ranked last (3.56, 71%), reflecting a weak technical understanding of encryption despite acknowledging its importance. The low standard deviation (0.68-1.02) indicates a homogeneity of opinions and strong consensus, reinforcing the positive relationship between the quality of protection and consumer trust.

Table No. (5) Analysis of the degree of agreement regarding the axes of organizational transparency in data use

Ranking	*Relative Importance*	*Standard Deviation*	*Arithmetic Mean*	*Statement*	
3	0,75	0,77	3,73	I appreciate organizations that clearly explain how they will use my personal data.	1
2	0,76	0,82	3,81	I prefer websites that indicate whether they will share my data with third parties (marketing companies, partners, etc.(.	2
5	0,73	0,76	3,66	I believe the organization should inform me of any changes to its privacy policy or data usage.	3
1	0,78	0,84	3,87	When a company explains the purposes for which it uses the data, I feel it is more credible.	4
6	0,72	0,88	3,60	I believe that concealing details of data usage reduces my trust in the organization.	5
7	0,72	0,86	3,59	I believe that providing a user control panel to manage privacy preferences increases the transparency of the organization.	6
4	0,74	0,80	3,71	The clearer the information provided about data usage, the more informed and reassuring my decision to use the platform was.	7
	0.74	**0.04**	**3.71**	**the total**	

Source: SPSS v26 output

Table (5) shows that the sample members agreed to a moderate to high degree on the principles of transparency, with an overall average of 3.71 out of 5. The fourth statement, "Clarifying the purposes for using data increases credibility," ranked first (3.87, 78%), indicating that basic transparency is the strongest factor in building trust. The second statement, "Disclosing data sharing with third parties," ranked second (3.81, 76%) due to participants' concerns about hidden marketing. The sixth statement, "A privacy management dashboard," ranked last (3.59, 72%) due to a lack of technical awareness of this tool, despite acknowledging its usefulness. The low standard deviation (0.76-0.88) indicates a convergence of opinions and agreement among participants on the importance of transparency as a fundamental condition for trust in digital platforms.

Table (6) Analysis of the Level of Agreement on Consumer Trust Axes

Ranking	*Relative Importance*	*Standard Deviation*	*Arithmetic Mean*	*Statement*	
2	0,78	0,65	3,87	I trust platforms that respect the privacy of my data and are committed to protecting it.	1
5	0,71	0,785	3,56	The organization's commitment to data ethics makes me more loyal to its brand.	2
6	0,7	0,82	3,51	When I feel confident about a particular platform, I am willing to share more personal data with it.	3
4	0,75	0,85	3,73	My confidence in an organization increases when I don't hear frequent complaints about data leaks or misuse.	4
1	0,78	0,84	3,92	If I have a good experience with a privacy-respecting platform, I recommend it to my friends and acquaintances.	5

3	0,76	0,79	3,78	My increased confidence in the platform makes me more willing to make repeat purchases from it.	6
7	0,69	0,90	3,42	If I lose trust in a platform due to data misuse, I will stop using it even if its services are good.	7
	0.73	**0.08**	**3.69**	**the total**	

Source: SPSS v26 output

Table (6) shows a strong relationship between data ethics and participant trust, with an overall mean of 3.69 out of 5. The fifth statement, "Recommending to others after a positive experience," ranked first (3.92, 78%), indicating the impact of social and behavioral trust. This was followed by the first statement, "Trust in privacy-respecting platforms" (3.87, 78%), which served as the basis for the ethical relationship. The seventh statement, "Stopping when trust is lost," ranked last (3.42, 69%), suggesting participants' reluctance to abandon services despite failures. The low standard deviation (0.65-0.90) reflects the convergence of opinions and their collective agreement that ethical commitment is a prerequisite for building sustainable trust and positive consumer behavior.

Testing the Hypotheses and Discussing the Results

-Hypothesis 1: There is a statistically significant relationship between data collection ethics and the consumer's perception of the level of privacy protection.

Table No. (07): The relationship between data collection ethics and consumer perception of the level of privacy protection

		Consumer awareness of the level of privacy protection	Data collection ethics
Consumer awareness of the level of privacy protection	Pearson Correlation	1	,871**
	Sig. (2-tailed)		,000
	N	190	190
Data collection ethics	Pearson Correlation	,871**	1
	Sig. (2-tailed)	,000	
	N	190	190

Source: SPSS v26 output

Table (7) shows a strong and statistically significant relationship ($r=0.871$, $p<0.001$) between data collection ethics and participants' perception of privacy protection. The high correlation coefficient indicates that 73.8% of the change in privacy perception is attributable to the level of ethical commitment in data collection. This demonstrates that transparency in informing consumers about the type of data being collected and obtaining their explicit consent enhances their sense of security and trust. Furthermore, the statistical significance level (Sig=0.000) less than 0.01 confirms that the relationship is not random. The results confirm that ethical commitment is essential for gaining the trust of digital consumers in commercial platforms, and this is supported by participants' agreement on the importance of clear reporting and explicit consent as the foundation of perceived privacy.

- Second Hypothesis: Organizational transparency in data use positively impacts consumer trust.

To test this hypothesis, appropriate statistical methods were used, namely correlation as a first step to determine the strength and nature of the relationship between institutional transparency in data use and consumer trust, followed by regression as a second step to determine the effect of the independent variable on the dependent variable.

Table (8) shows the results of the simple linear regression analysis for the second hypothesis.

Results of the analysis of the relationship between institutional transparency in data use and consumer trust		
0.731	Pearson correlation coefficient R	Study methods

0.000			Significance probability value (sig(		
Results of simple regression analysis to measure the impact of institutional transparency on data use and consumer trust					
Coefficient of determination (R2) 0.535, standard error of estimation 0.52811					
F-value: 59.053, Significance level: 0.00					
moral T	value T	β	SE	B	variable
0.000	6.220		0.182	1.130	The constant
0.000	13.723	0.731	0.052	0.713	Follower

Source: SPSS v26 output

Institutional transparency in data use leads to increased consumer trust. To test this hypothesis, we used appropriate statistical methods, beginning with correlation analysis to determine the strength of the relationship between institutional transparency and consumer trust. The results showed a Pearson coefficient of 0.731, indicating a strong positive correlation between the two variables; that is, increased institutional transparency is associated with increased consumer trust. The p-value was 0.000, indicating strong statistical significance. Subsequently, we used simple linear regression to measure the impact of institutional transparency on consumer trust. The results showed a coefficient of determination (R^2) of 0.535, meaning that 53.5% of the change in consumer trust can be explained by institutional transparency, confirming that transparency significantly contributes to increased trust. The F-value was approximately 59.053 with a significance level of 0.00, confirming the statistical significance of the model. For the independent variable (organizational transparency), the regression coefficient B was 0.713, and the t-value was 13.723, indicating a strong and statistically significant effect of transparency. With a p-value of 0.000 (less than 0.05), the effect is statistically significant. Ultimately, the results confirm that organizational transparency in data use has a strong and positive impact on consumer trust, supporting the hypothesis.

-Hypothesis 3: There is a statistically significant relationship between organizational privacy policies and enhancing consumer loyalty and brand trust.

Table (9): The relationship between data collection ethics and consumer perception of the level of privacy protection .

Source: SPSS v26 output

		Consumer loyalty and trust in the brand	Privacy Protection Policies
Consumer loyalty and trust in the brand	Pearson Correlation	1	,799**
	Sig. (2-tailed)		,000
	N	190	190
Privacy Protection Policies	Pearson Correlation	,799**	1
	Sig. (2-tailed)	,000	
	N	190	190

Table (9) shows a strong and statistically significant relationship (r=0.799, p<0.001) between privacy policies and brand loyalty. These policies explain 63.8% of the variance in loyalty levels, indicating that investing in strong encryption, enabling data deletion, and transparency with third parties helps build a long-term strategic relationship. The significance level (Sig=0.000) confirms that the results are not random and demonstrates that privacy policies enhance trust, leading to repeat purchases, social recommendations, and brand loyalty. Therefore, it is crucial to allocate resources to strengthen digital security as a competitive priority for Algerian platforms.

Discussion and Interpretation of Results

Hypothesis 1: There is a statistically significant relationship between data collection ethics and consumer perception of privacy protection.

The results showed a strong correlation between data collection ethics and consumer perception of privacy protection (r=0.871, p<0.001), with transparency in informing consumers and obtaining their explicit consent explaining 73.8%

of this perception. This aligns with privacy protection theory, where consumers weigh the benefits against the risks before sharing their data. The results underscore the importance of ethical commitment in building trust at the outset of digital interaction and support the principle of informed consent as the foundation for the relationship between organizations and consumers in Algeria. The results also demonstrate that ethical transparency is more important than technical aspects in the consumer's view, highlighting the need to train employees in clear disclosure within the culture of digital platforms.

Hypothesis 2: Organizational transparency in data use positively impacts consumer trust.

The results showed that transparency has a strong and positive impact on consumer trust, with the statement "Clarifying the purposes for using data increases credibility" receiving the highest average score (3.87 out of 5). This demonstrates that disclosing data sharing with third parties and reporting policy changes enhances an organization's credibility. This finding aligns with the modified SERVQUAL model for the digital context, where transparency is considered a fundamental element of service quality. Participants demonstrated a high sensitivity to secrecy, which erodes trust, and emphasized that clarity is essential for maintaining relationships. The results support organizations' investment in user dashboards as a transparency tool that meets the expectations of Generation Z and highlight the importance of developing real-time notification systems when data policies change. The findings also support the principle of shared responsibility between organizations and consumers.

Third Hypothesis: There is a statistically significant relationship between organizational privacy policies and enhancing consumer loyalty and brand trust.

The results showed a strong correlation between privacy policies and consumer loyalty ($r=0.799$, $p<0.001$), with "recommendation to others" being the most prominent behavior resulting from trust based on technical security. The results explain 63.8% of the loyalty variance by the effectiveness of encryption and the right to delete, confirming that security can become a moral value for the organization. These results are consistent with the sustainability theory, where loyalty is built on repeated positive experiences. They also justify organizations' investment in advanced security systems as a long-term competitive advantage and highlight the importance of developing a digital security culture as part of the brand identity. Furthermore, they underscore the necessity of training employees in ethical principles.

Study Recommendations and Suggestions

Enhancing trust and transparency in data ethics on digital platforms requires practical steps, such as developing clear policies, providing technical tools, organizing awareness campaigns, and enacting national legislation. Further, more extensive future research is also suggested. The most important recommendations can be summarized as follows:

•Concise and clear privacy policies should be developed in simple language, explaining the types of data collected, their uses, and the beneficiaries.

•It is important to provide users with control panels that allow them to manage their preferences, delete their data, and opt out of collecting certain information.

•Investing in advanced encryption systems and obtaining certified security information should enhance technical trust.

•Awareness campaigns should be launched in Algeria to explain privacy violations and how to address them.

•Legislation should be enacted to protect data, mandating explicit user consent.

•Digital privacy oversight bodies should be established to penalize violators. 8. Conclusion

This study indicates that data ethics are essential for building consumer trust in digital platforms in Algeria. The results also demonstrate a strong correlation between transparency and user loyalty, underscoring its importance. With the accelerating digital transformation in Algeria and globally, adherence to these ethics becomes a competitive advantage that strengthens platforms' market position. The findings highlight the need for clear privacy policies and advanced protection tools to bridge gaps in awareness and implementation. Furthermore, there is a need for national legislation inspired by global best practices to protect data and ensure informed consent. By implementing the recommendations, platforms can transform privacy into an investment that fosters user loyalty and protects the brand. The study emphasizes the importance of future research, including comparative and long-term studies, to broaden the geographical and age-based scope. Data ethics represents a bridge to a sustainable digital economy that balances innovation and responsibility. Trust is paramount, and its loss threatens the growth of any sector. Therefore, the research calls for immediate collaboration between platforms, legislators, and society to ensure a safe and trustworthy digital environment.

Ethical Considerations

This study was conducted in full accordance with recognized ethical standards for social science research involving human participants. Participation in the survey was entirely voluntary, and all respondents were informed in advance about the purpose of the study, the nature of the data collected, and their right to withdraw at any time without consequence. Informed consent was obtained from all participants prior to data collection. The questionnaire was designed to avoid sensitive or personally identifiable information, and all responses were collected anonymously. Data confidentiality and privacy were strictly maintained throughout the research process, and the collected data were used exclusively for academic and scientific purposes. The study complied with general principles of data protection and ethical research conduct, including respect for participants' privacy, transparency, and responsible data handling.

Acknowledgements

The author would like to express sincere gratitude to all participants who generously contributed their time and insights to this research. Appreciation is also extended to colleagues at Ferhat Abbas Sétif University 1 for their academic support and constructive feedback during the development of this study.

Funding

This research received no external funding and was conducted independently by the author.

Conflict of Interest

The author declares that there is no conflict of interest regarding the publication of this paper. The research was carried out without any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Helen Nissenbaum. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
2. Luciano Floridi. (2013). The Ethics of Information. Oxford University Press.
3. Solove, D. (2008). Understanding Privacy. Harvard University Press.
4. Thomas C. Redman. (2013). Data driven: Profiting from your most important business asset. Harvard Business Press.
5. Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. Science, 366(6464).
6. Asala Bouali and Tawfiq Abidi. (2025). Research ethics in the digital age. Guelma, Algeria: Journal of Cultural Dialogue, Vol. 14, No. 1.
7. Jamila Boudaoud. (2013). The impact of brand image on consumer behavior. Algeria: Maaref, a peer-reviewed scientific journal, Volume 8, Issue 14.
8. Hamid Laboukh. (2025). Ethical Artificial Intelligence and Data Privacy in Islamic Financial Technology. Oran, Algeria: Journal of Studies in Islamic Finance and Development, Volume 6, Issue 11.
9. Samia Boussaâd. (2022). Protecting Consumers' Personal Data from the Risks of Electronic Payments. Algeria: Journal of Law and Human Sciences, Volume 15, Issue 1.
10. Samia Chenar and Abdelwahab Meddassi. (2020). Research Ethics in Light of Technological Development. Batna, Algeria: Journal of Sociology, Volume 4, Issue 2.
11. Aicha Mostafa Benkara. (2019). Mechanisms for Protecting Personal Data in Algerian Legislation According to the Provisions of Law (0.7-18). Algeria: Journal of Legal and Political Sciences, Volume 10, Issue 1.
12. Abdallah Nour Eddine and Mohamed Ben Adda. (2023). Methodological Frameworks and Ethical Issues in Data Collection and Analysis. Algeria: Journal of Organization and Work, Volume 11, Issue 4.
13. Gharib Taous. (2022). Commitments to Digital Marketing Ethics and Their Role in Consumer Protection: A Study of a Sample of Consumers. Tebessa, Algeria: Journal of Finance and Markets.

14. Karima Ben Sghir, Malika El Afri, and Amira Hamel. (2021). A Reading of the Ethical Values of the Fundamentals of Scientific Research. Guelma, Algeria: Ansaniyat Journal of Research and Studies, Volume 12, Issue 2.
15. Lahcen Attallah. (2019). The Impact of Marketing Ethics on Customer Loyalty to a Brand with Satisfaction as a Mediating Variable: A Case Study of the Condor Brand. Algeria: Al-Muntada Journal of Economic Studies and Research, Volume 3, Issue 1.
16. Maamar Ben Ali and Abdelmalek Dah. (2020). Guaranteeing the Rights of the Online Consumer within the Framework of Their Personal Data. Laghouat, Algeria: Academic Journal of Legal and Political Research, Volume 4, Issue 1.
17. Najat Bouam and Sami Amri. (2020). Ethical guidelines for research in the humanities. Algeria: Journal of Humanities, University Center of Ali Kafi Tindouf, Volume 4, Issue 1.