

TRUST MODELS AND DATA PRIVACY IN E-COMMERCE: A CASE STUDY OF JUMIA KENYA

FW Otinga, Maseno University
HA Khazalwa, Maseno University
FO Aila, Maseno University

ABSTRACT

The proliferation of E-commerce significantly transforms trade, connecting businesses and consumers in novel ways. In Kenya, Jumia, a leading online marketplace, exemplifies this transformation. However, the rapid growth of E-commerce platforms raises critical concerns about trust, security, and data privacy. Customers are wary of sharing personal details due to potential misuse and a lack of awareness about privacy settings, secure practices, and possible risks. Our paper investigates the effectiveness of trust-building mechanisms and data privacy through a qualitative approach, including a systematic literature review and case study analysis. Our findings highlight the importance of robust security measures, transparent policies, and user-friendly design in fostering consumer trust. In conclusion, while Jumia Kenya's practices align well with best practices, continuously enhancing data privacy measures is necessary to address evolving user concerns. We recommend increasing transparency in data handling, enhancing user education on privacy settings, and regularly updating security protocols. Our paper is relevant to managers, government bodies, academicians, and other stakeholders who shape e-commerce policies in Kenya, emphasizing the need for robust trust, security, and privacy measures to foster successful online business relationships.

Keywords: E-commerce, trust, data privacy, Jumia Kenya.

INTRODUCTION

E-commerce is traced back to the 1960s when businesses started using Electronic Data Interchange (EDI) to exchange business documents electronically. However, it was in the 1990s that e-commerce truly began to take shape with the emergence of the World Wide Web (Schwandt, 1997). Over the past few decades, e-commerce has grown exponentially due to technological advancements and changes in consumer behavior. E-commerce, short for electronic commerce, encompasses a wide range of business activities online. It involves exchanging information or monetary transactions (or both) using digital platforms leveraging the power of the web to facilitate commercial interactions among organizations and individuals (Ferrera & Kessedjian, 2019).

E-commerce offers consumers 24/7 availability, lower prices, global reach, and convenience in various business settings. The increasing Internet and mobile penetration and the growing consumer adoption of online payments have contributed to the growth of Kenya's e-commerce landscape. Customers are more involved with online shopping, and mobile payment has enabled more accessible and faster e-commerce orders (Turban et al. 2017).

Kenya is amongst the fastest-growing e-commerce markets in Africa, with more than ten online retailers. Jumia, which started in Nigeria twelve years ago and is now publicly listed on the New York Stock Exchange, is Kenya's leading e-commerce market, with over one-fifth of the market share. Known as the "African Amazon," its online marketplace connects thousands of sellers with consumers. It offers a wide range of branded and non-branded affordable and quality consumer goods, such as fashion and apparel, beauty products, electronics, and home and living. However, as e-commerce grows, trust, security, and privacy concerns emerge (Chebichiy & Odhiambo, 2020). Consumer distrust is a significant concern in e-commerce, primarily revolving around protecting private information and the fear of exposure to fraudulent online activities. For consumers to engage confidently in online

transactions, trustworthiness becomes paramount. Therefore, we scrutinize the various trust models and data privacy mechanisms used by Jumia to protect consumer-sensitive data from third-party access.

Background of the Study

The Internet revolution has fundamentally transformed how businesses operate, offering unprecedented opportunities for commerce through digital platforms (Zerbini et al., 2020). E-commerce, in particular, has emerged as a powerful driver of economic growth, enabling businesses to reach a global customer base with ease. In Kenya, Jumia Kenya stands out as a leading e-commerce platform exemplifying both the potential and challenges of this digital marketplace. Despite its success, Jumia Kenya, like many e-commerce platforms, faces critical issues related to trust, security, and data privacy. These concerns are paramount as they significantly influence consumer behavior and the overall sustainability of online businesses. Our paper investigates how Jumia Kenya addresses these challenges and provide insights into effective trust models and data privacy practices in the e-commerce sector.

Trust is a fundamental element in e-commerce; without it, consumers are hesitant to engage in online transactions (Gefen, 2000). Issues such as the protection of personal information, the risk of data breaches, and the potential misuse of data are significant barriers to building trust (Hoffman, Novak & Peralta, 1999). In the Kenyan context, these concerns are impaired by the evolving nature of data privacy laws and varying levels of consumer awareness about online security (Mwangi, 2021). The existing literature on e-commerce emphasizes the critical role of trust in online transactions. Trust models in e-commerce often incorporate reputation systems, security measures, and transparency to build consumer confidence (Pavlou, 2003). Data privacy is equally crucial, with consumers increasingly concerned about the security of their personal and financial information (Chellappa & Pavlou, 2002). Regulatory frameworks, such as the General Data Protection Regulation (GDPR) and Kenya's Data Protection Act (2019), set standards for data privacy. The literature review identifies best practices in trust and data privacy, forming the basis for our case study of Jumia Kenya.

We aim to bridge the gap between theoretical models of trust and data privacy and their practical implementation within Jumia Kenya. By combining a systematic literature review with a detailed case study, we provide a comprehensive understanding of how trust can be effectively built and maintained in e-commerce. Our case study of Jumia Kenya offers a unique perspective, highlighting the strategies and practices that have contributed to its growth and popularity among consumers in ensuring data privacy and security.

Justification of the Study

As e-commerce continues to grow exponentially, understanding the mechanisms that foster trust and ensure data privacy is crucial for both academic inquiry and practical application.

Addressing Trust in E-commerce

Trust is a fundamental element in the success of e-commerce platforms. Consumers' willingness to engage in online transactions is heavily influenced by their trust in the platform. The e-commerce industry grapples with significant trust, security, and privacy issues with consumers frequently expressing concerns about safeguarding their personal information and the potential risk of online fraud hence insights from Jumia's experiences illuminate these challenges and offer possible solutions. While establishing trust with consumers is vital; Jumia's trajectory offers valuable insights into how an e-commerce platform mitigates consumer distrust and strengthens trustworthiness (Okeke et al. 2013). By examining Jumia Kenya, our paper provides valuable insights into practical trust-building mechanisms such as reputation systems, security measures, user experience, and transparency. Our findings guide other e-commerce platforms in developing strategies to enhance consumer trust, ultimately leading to increased customer loyalty and sustained business growth.

Enhancing Data Privacy Practices

Data privacy is an increasingly important issue in the digital age. With the increase of data breaches and growing concerns over personal data misuse, e-commerce platforms must implement robust data privacy practices to protect users. Jumia's operations involve managing sensitive data, encompassing personal details and financial transactions, and studying its practices reveals how it addresses security and privacy concerns. We examined Jumia Kenya's data privacy practices, including data collection, storage, sharing, and regulatory compliance. By highlighting effective practices, we contribute to the broader discourse on data privacy in e-commerce. Our findings inform policymakers, regulators, and platform managers about best practices and potential pitfalls in data privacy management, ensuring that user data is handled responsibly and securely.

Regional Relevance and Contribution

Most existing research on e-commerce trust and data privacy focuses on platforms in developed markets such as North America and Europe. Our study fills a gap by focusing on Jumia Kenya, providing insights into the unique challenges and opportunities in the African e-commerce landscape. The regional relevance of our research is significant, as it offers context-specific findings applied to similar markets in developing regions. We contribute to a more comprehensive understanding of e-commerce dynamics globally and support the development of tailored strategies for platforms operating in diverse environments.

Empirical Evidence and Practical Application

The integration of systematic literature review findings with empirical data from Jumia Kenya offers a robust framework for understanding the interplay between theoretical models and real-world practices. This empirical evidence is crucial for validating existing theories and developing new ones that reflect the complexities of modern e-commerce. The practical application of our findings is immense, as they provide actionable insights for e-commerce platform managers, helping them to implement effective trust-building and data privacy measures. Our study's recommendations guide future research, encouraging scholars to explore similar issues in different contexts and with different methodologies.

Supporting Regulatory Frameworks

As governments and regulatory bodies worldwide continue to develop and enforce data protection laws, our study offers timely insights into how e-commerce platforms align with regulatory requirements. Examining Jumia Kenya's compliance with local and international data protection standards, the research provides a benchmark for other platforms aiming to enhance their regulatory compliance. This is particularly relevant in the context of the Kenyan Data Protection Act (2019) and the General Data Protection Regulation (GDPR), which set high standards for data privacy and protection. Jumia's experiences guide policymakers, academics, and other stakeholders in formulating policies and regulations for e-commerce in Kenya. By scrutinizing Jumia's practices, we propose effective strategies to support regulatory policies.

Problem Statement

As e-commerce platforms expand, issues related to trust and data privacy become increasingly significant. Despite the potential benefits of online shopping, consumers often hesitate to engage in e-commerce due to concerns about trustworthiness and the security of their data. This hesitation is attributed to various factors, including the fear of fraud, data breaches, and misuse of personal information. Understanding how to effectively build and maintain trust, while ensuring robust data privacy practices, is crucial for the success of e-commerce platforms. The existing literature provides various models and best practices for trust-building and data privacy, but there is a lack of awareness

on how these models are implemented and perceived in specific regional contexts, such as Kenya. Moreover, regulatory environments and consumer expectations vary significantly across different markets, necessitating a localized approach to these issues.

Research Objectives

Our primary aim is to investigate trust models and data privacy practices in the context of Jumia Kenya. We seek to understand how trust is established, maintained, and impacted by privacy-related factors. Our objectives are as follows;

1. To investigate and analyze existing trust-building mechanisms employed by e-commerce platforms with a focus on Jumia Kenya. We assess how Jumia Kenya implements various trust-building mechanisms.
2. To understand how Jumia Kenya handles sensitive customer information i.e. examining the data collection, storage, and sharing practices employed by Jumia Kenya.

Research Questions.

In the dynamic landscape of e-commerce, trust plays a pivotal role in shaping consumer behavior and fostering sustainable relationships between online platforms and their users. As digital transactions become increasingly prevalent, understanding the intricate interplay between trust-building mechanisms and data privacy practices becomes paramount. Our research examines Jumia's experiences in unraveling the following critical research questions;

1. What are the existing trust-building mechanisms employed by Jumia Kenya?
2. What data privacy practices does Jumia Kenya employ, and how do they align with best practices and regulatory requirements? What privacy protocols and safeguards are in place to protect user data? How do these practices intersect with trust dynamics?

Research Significance

In the ever-evolving landscape of digital commerce, the delicate balance between trust and data privacy emerges as a critical concern. As consumers increasingly rely on e-commerce platforms for their shopping needs, understanding the complex dynamics that shape trust and privacy practices becomes vital. Trust is the bedrock upon which successful e-commerce transactions are built and investigating how Jumia Kenya establishes and nurtures consumer trust sheds light on strategies that resonate with online shoppers. The handling of sensitive customer information is a delicate dance between convenience and security, hence, examining Jumia's data privacy practices, provides insights into how e-commerce platforms strike a balance, ensuring user confidence while safeguarding personal data.

Our findings have broader implications for the e-commerce industry. As businesses navigate the complexities of privacy regulations, understanding Jumia's experiences inform best practices and policy recommendations. Jumia's operations in Kenya provide a unique lens into the African market contextualizing trust and privacy within this regional context, contributing to a deeper understanding of e-commerce dynamics in Africa.

METHODOLOGY

Research Approach

We adopted a qualitative research design to study the trust models and data privacy in E-commerce combining the Systematic Literature Review and Case study analysis of Jumia Kenya.

Systematic Literature Review

We carried out a comprehensive search of the database, that is, Google Scholar, for peer-reviewed articles related to trust models, data privacy, and E-commerce. Our search was guided by specific keywords: "Trust models AND Data privacy, E-commerce," and "Jumia Kenya." Our

inclusion and exclusion criteria were clearly defined to ensure our rigor and reproducibility. The inclusion criteria narrowed to studies published between 2019 and the present, focusing on trust models, data privacy, and e-commerce. The articles available in English, accessible in PDF format, and open access were considered. The exclusion criteria consist of studies published before 2019, not available in English, lacking PDF accessibility, and having restricted access. Additionally, studies that do not utilize the specified keywords were removed.

In the context of our research, we extracted relevant information from the selected studies which included understanding the study's purpose, examining its methodology, analyzing the findings, and considering the implications for trust models and data privacy in the realm of e-commerce.

Case Study of Jumia Kenya

We analyzed the company's data privacy policies and practices, customer reviews, and any available reports on data breaches or privacy issues from its platform (<https://www.jumia.co.ke>). We aimed to understand how trust models and data privacy are implemented in Jumia Kenya and how these impact customer trust and satisfaction. Jumia Kenya operates in a region where E-commerce proliferates, with online companies mushrooming everywhere. This growth presents numerous business opportunities and challenges that can be explored through our case study. Consumer distrust, mainly regarded as protecting private information, and the fear of being exposed to fraudulent online activities pose a significant obstacle to e-commerce in Kenya. Studying Jumia Kenya provides insights into these issues and potential solutions. The company operates in an environment where data privacy laws and regulations are still evolving, offering an opportunity to study how an E-commerce company navigates data privacy issues in such a context. Additionally, Jumia Kenya, preferred by most consumers in the country, serves as a successful case study, providing valuable insights into effective trust models in E-commerce.

RESULTS AND DISCUSSION

Systematic Literature Review

A total of 436 articles were identified from Google Scholar containing the specific keywords and after screening, and filtering, 16 articles were downloaded. From this, 9 articles were relevant to our study as per Figure 1.

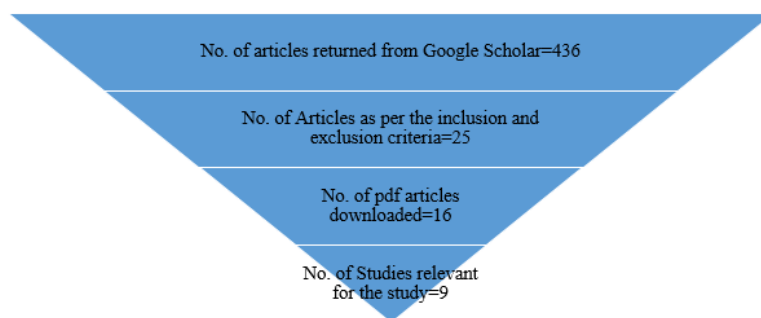


FIGURE 1
SYSTEMATIC LITERATURE REVIEW

Our key findings are highlighted in Table 1.

Table 1					
Author	Year	Method(s)	Key Findings	Article Name	Field of Study
Jabar, A. A., & Ogunsola, A	2022	Analytical	Opportunities and challenges in e-commerce. The slow acceptance of e-commerce and decline in their use due to cybercrimes and	Analytical Review of E-Commerce	Business Development

			other related internet-related fraudulent activities. Recommends business owners to procure quality devices and gadgets that will enhance efficiency, adopt models that fit well in their business without compromising user security.	Business Models	
Saidu, M. A., Shamsudeen, L. S., Muhammad, A. K., & Abdulkadir, A	2022	Exploratory	E-commerce platforms and data security. Users are skeptical about using applications for fear of data breaches. Cyber-attacks increase with an increase in e-commerce platforms trading. Recommends block-chain database management system to help control cyber-attacks in e-commerce without third party's involvement.	Exploring E-Commerce Opportunities for a Better International Trading and Tax Revenue Generation: A Review for Developing Countries.	Technology
Daramola, O., & Etim, E.	2022	Analytical	Provides an analytical review of technological affordances of digital platforms in Sub-Saharan Africa. Insights into the imperatives for designing inclusive and accessible digital platforms for the informal sector. Trust building through reviews and rating of services. Recommends governments to regulate health and safety issues concerning customers and service providers to be prioritized. (Collaboration among stakeholders).	Affordances of digital platforms in sub-Saharan Africa: An analytical review.	Technology
Osita, G. C., Chisom, C. D., Okoronkwo, M. C., Esther, U. N., & Vanessa, N. C.	2022	Qualitative	Security remains a major challenge to the success and survival of e-commerce businesses globally. Emerging technologies significantly contribute to the mitigation of security concerns in e-commerce by providing innovative solutions to combat cyber threats, fraud, data breaches, and unauthorized access.	Application of Emerging Technologies in Mitigation of E-Commerce Security Challenges.	E-commerce
Zaidan, M. N., & Raju, V.	2021	Mixed	Primary relevance on conceptual model based on characteristics that influence online purchasing intentions, with an emphasis on perceived trust and perceived security, as well as attitudes.	Literature review of factors affecting the online purchase intention in Iraq.	E-commerce
Tidjani, C	2021	Exploratory	Data and privacy security are identified as obstacles to the successful adoption of Fin-Tech business in the North African region. Recommends regulatory framework for private data access and technological infrastructure.	COVID-19 and challenges of the Fintech industry: A state of the art and outlooks on the North African region.	Technology
Tian, W.	2022	Mixed	Recent development of e-commerce platforms in emerging markets, and defines e-commerce platforms broadly and summarizes their various characteristics. Highlights opportunities and challenges of e-commerce including data privacy and trust.	E-commerce Platform in the Global South—Concepts, Trends, and Cases.	E-commerce
Olubusola, O.,	2024	Comparative	Unique understanding of the opportunities and challenges of digital transformation in	Digital transformation in	Business Development

Mhlongo, N. Z., Falaiye, T., Ajayi-Nifise, A. O., & Daraojimba, E. R.		the USA and Africa. Invest in robust cyber security measures addressing the skill gaps through training programmes and fostering a culture of adaptability to stay ahead of technological advancements.	business development: A comparative review of USA and Africa.	
---	--	---	---	--

Our review highlights consumer distrust as a major concern, mainly regarding the protection of private information and the fear of being exposed to online fraudulent activities in e-commerce. The studies provide recommendations to foster a healthy online environment for both consumers and businesses.

Case Study Findings

Reputation Systems

Our case study analysis reveals that Jumia Kenya effectively uses reputation systems to build consumer trust. User reviews and ratings play a significant role in influencing purchasing decisions, underscoring the importance of maintaining high service standards to enhance user experience.



FIGURE 2
JUMIA LANDING PAGE

Security Measures

Jumia Kenya’s robust security measures, including encryption and secure payment gateways, align with best practices. These measures are critical in mitigating risks associated with online transactions and enhancing consumer trust. Strict verification procedures are applied to these payment types to guarantee transaction legitimacy and guard against fraud.

User Experience

The platform’s user-friendly design positively impacts consumer trust. Easy navigation, clear product descriptions, and efficient customer service contribute to a seamless shopping experience, reinforcing trust.

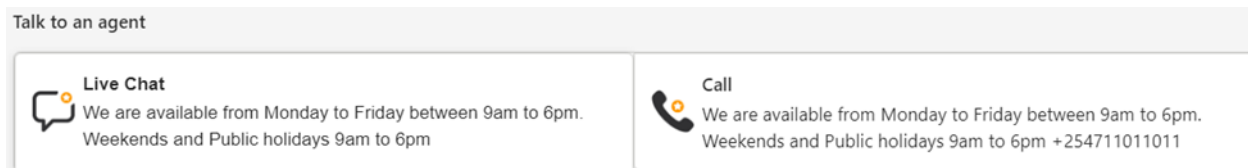


FIGURE 3
CUSTOMER SUPPORT CONTACT

Transparency and Policies/Consent Management

Clear communication of privacy policies and data handling practices is essential for maintaining trust. Jumia Kenya's transparency in these areas, coupled with adherence to regulatory requirements, enhances consumer confidence.

Identity Verification

Jumia uses both pre-requisite and in-session steps to set up user authentication. Since the nature of the user registration process and the provider of user credentials are vital to establishing identity, Jumia requires registration for users who intend to fulfill transactions that fall within the range of its definition of sensitive data categories. During registration, users are prompted to provide specific identification data and create an account with a corresponding username and password. Account data is stored as defined and may be used to re-establish verified identity in subsequent sessions. Passwords are stored in a manner that Jumia administrators cannot access. During subsequent visits, the username and password combination is used to gain access to higher-level account functionalities.

Buyer Protection Programme

Jumia has put in place a Return Policy to give users an additional degree of security. This programme guarantees that customers will receive the things they request and that the quality will be guaranteed. Jumia safeguards customers' interests and fosters platform trust by providing a refund or replacement if there are issues with the order.

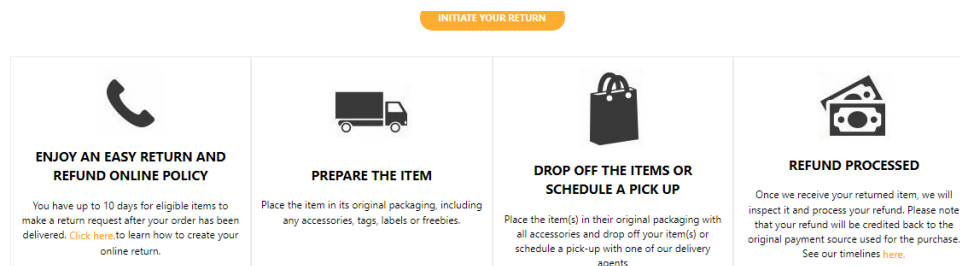


FIGURE 4
JUMIA RETURN POLICY

Partnership and Third-Party Services

Working with reliable partners allows Jumia to further strengthen the security ecosystem of its platform. Jumia carefully selects and partners with trusted third-party services and providers to enhance the security of its platform. These partners go through rigorous evaluation processes to ensure that they meet Jumia's security and privacy standards.

Adidas	Cantu	Epson	Intel	Maybelline	Ramtons	Sony	USN
ALLVONS	Coke	Garrier	Jameson	Mika	Roch	TCL	Vision Plus
Apple	DELL	Hisense	L'Oréal Paris	NIVEA	Samsung	Tecno	Vitron
Asus	Dove	HP	Lenovo	Nunix	Sandisk	Transcend	VON
Bruhnn	Dr. Rashel	Infinix	Logitech	Oppo	Skyworth	Tusker	XIAOMI
Canon							

FIGURE 5
JUMIA PARTNERS

Data Protection Policy

Jumia has put in place extensive data protection guidelines to secure the private and corporate data that it collects from customers, employees, and entrepreneurs. These rules describe the steps Jumia has taken to guarantee that data is gathered, maintained securely, and used exclusively for the purposes for which it was intended (<https://www.jumia.co.ke/sp-privacy/>). Jumia complies with applicable data protection laws and regulations as per the Kenya Data Protection Act.

Encryption and Authentication

Jumia uses advanced encryption techniques to safeguard user data while it is being transported between its platform and users. This guarantees that all transmitted data, including login credentials, payment information, and client details, is safely encrypted and impenetrable to third parties. To guarantee that only those with permission access the platform and its services, Jumia employs robust user authentication and access controls. Role-based access controls, password regulations, and multi-factor authentication are some examples of this. These safeguards assist in preventing unwanted access to private information and safeguard startup and entrepreneur accounts.

Trust Models in Jumia Kenya

The literature highlights several key mechanisms for building trust in e-commerce, including reputation systems, security measures, user experience, and transparency. Our findings reveal that Jumia Kenya's approach aligns well with these models. The platform's comprehensive rating and review system mirrors the reputation systems (Daramola and Etim, 2022). By enabling customers to share their experiences and rate products and sellers, Jumia Kenya helps potential buyers make informed decisions, thereby enhancing overall trust.

Security measures are another critical component identified in the literature. Jumia Kenya's use of HTTPS for secure transactions, along with advanced encryption techniques, aligns with best practices for protecting user data (Olubusola *et al.*, 2024; Oista *et al.*, 2022; Said *et al.*, 2022). This focus on security not only protects sensitive information but also reassures users about the safety of their transactions on the platform.

User experience, as emphasized in the literature, is also a significant trust factor. Jumia's intuitive website and mobile app design, efficient order tracking, and responsive customer service contribute to a positive user experience, reinforcing the findings of research on the impact of user-friendly interfaces on trust (Zaidan and Raju, 2021).

Transparency and clear communication of policies are critical for maintaining trust (Jabar & Olunsola, 2021). Jumia Kenya's clear privacy policies and terms of service, which are readily accessible to users, demonstrate a commitment to transparency and reinforce the platform's trustworthiness.

Data Privacy Practices

Data privacy is another cornerstone of trust in e-commerce, encompassing data collection, storage, sharing, and regulatory compliance. Jumia Kenya's practices confirm the importance of these aspects, as outlined in the literature. The platform's approach to data collection, which involves

gathering only necessary information, aligns with the principle of data minimization advocated in privacy guidelines such as the GDPR *i.e. General Data Protection Regulation* (Tidjani, 2021).

Secure data storage is crucial to prevent breaches and unauthorized access. Jumia Kenya's use of secure servers and encryption protocols reflects best practices in the field, addressing concerns highlighted by previous research (Jabar & Olunsola, 2021). Furthermore, limiting data sharing to trusted third-party service providers and ensuring their compliance with data protection standards aligns with recommendations for maintaining user trust through controlled data sharing (Saidu et al., 2022).

Regulatory compliance is essential for protecting user data and fostering trust. Our findings reveal that Jumia Kenya's adherence to Kenyan data protection laws and alignment with international standards such as the GDPR demonstrates a proactive approach to regulatory compliance. This commitment not only ensures legal compliance but also enhances the platform's credibility and trustworthiness (Daramola & Etim, 2022).

CONCLUSIONS

Jumia Kenya has implemented effective trust models and data privacy practices, contributing to its reputation as a trustworthy e-commerce platform. Continuous improvements in security measures, transparency, and regulatory compliance are essential to maintain and enhance user trust. Addressing user concerns and adapting to evolving data privacy standards will be crucial for Jumia Kenya's sustained success in the competitive e-commerce landscape. The integration of systematic literature review findings with case study insights from Jumia Kenya reveals a strong alignment between theoretical models and practical implementations. Reputation systems emerge as a key component in building trust within e-commerce platforms. Both the literature and the case study findings confirm that effective reputation systems, like Jumia Kenya's rating and review mechanism, play a crucial role in establishing and maintaining consumer trust. These systems provide valuable feedback that helps users make informed purchasing decisions, thereby enhancing their overall confidence in the platform.

Security measures are another critical aspect where Jumia Kenya aligns well with the best practices discussed in the literature. The platform's implementation of HTTPS for secure transactions and advanced encryption techniques exemplifies the robust security measures necessary to protect user data and maintain high levels of trust. This alignment with theoretical models underscores the importance of strong security protocols in fostering a trustworthy e-commerce environment.

The user experience on Jumia Kenya also reflects the best practices identified in the literature. The positive impact of a user-friendly design on customer trust is evident in both theoretical frameworks and empirical findings from the case study. Jumia's focus on creating an intuitive, easy-to-navigate website and mobile app significantly enhances user satisfaction and trust. This consistency between literature and practical application highlights the critical role of user experience in the success of e-commerce platforms.

Transparency and policies regarding data privacy are crucial for maintaining trust, and Jumia Kenya's practices align with these theoretical insights. The clear communication of privacy policies and transparent data handling practices, as evidenced in both the literature and the case study, is essential for building and sustaining consumer trust. By adhering to these principles, Jumia Kenya ensures that users feel secure and informed about how their data is being managed, reinforcing the overall trust in the platform.

RECOMMENDATIONS

The digital landscape of e-commerce is continuously evolving, presenting both opportunities and challenges. As a leading e-commerce platform in Africa, Jumia Kenya must navigate these changes

to maintain and enhance user trust and data privacy. Effective strategies in data security, transparency, and regulatory compliance are essential to ensure a secure and trustworthy online shopping experience. Our research offers valuable insights into a healthy online business environment for all the stakeholders.

For platform managers, it is crucial to enhance data security by implementing regular updates and audits of security protocols to guard against emerging cyber threats. Investing in advanced encryption technologies and ensuring secure data storage and processing are paramount. Improving transparency involves providing detailed explanations of data handling practices and timely updates to privacy policies. Enhancing communication channels to keep users informed about any changes or data-related incidents is also essential. Additionally, developing robust mechanisms for users to report and resolve data privacy concerns efficiently is important, as incorporating user feedback will continuously improve data privacy and security practices.

Customers should stay informed by regularly reviewing Jumia's privacy policies and updates to understand how their data is used and the measures in place to protect it. Utilizing available security features such as two-factor authentication for account protection and regularly updating passwords is advised. Customers should also be cautious about sharing personal information. Actively participating in surveys and feedback mechanisms provided by Jumia to voice any concerns about data privacy and security is vital, as customer input helps improve the platform's practices.

Policy regulators should focus on strengthening regulations by developing and enforcing robust data protection laws that align with international standards, ensuring these regulations address emerging threats and technologies in the e-commerce space. Regularly auditing e-commerce platforms like Jumia to ensure compliance with data protection laws and providing clear guidelines and support for companies to adhere to these regulations is crucial. Additionally, public awareness campaigns to educate the public on their data privacy rights and the importance of data security are needed, promoting best practices for personal data protection in the digital age.

Moreover, in academia, conducting in-depth research on trust models and data privacy practices in e-commerce is essential, with a focus on emerging trends, potential vulnerabilities, and innovative solutions to enhance data security and user trust. Integrating topics on e-commerce security, data privacy, and trust models into academic curricula will prepare future professionals with the knowledge and skills needed to address these critical issues. Partnering with e-commerce platforms like Jumia for research projects, internships, and case studies provides valuable real-world insights and contributes to the development of best practices in the industry.

REFERENCES

- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3-4), 245-270.
- Chebichiy, R., & Odhiambo, E. (2020). Challenges and opportunities of e-commerce in Kenya: A case study of Jumia Kenya. In *Rethinking Sustainable Development Goals in Africa: Emerging Trends and Issues*, 1(1), 188.
- Ferrero, C., & Kessedjian, E. (2019). Evolution of e-commerce and global marketing. *International Journal of Technology for Business (IJTB)*, 1(1), 33–38.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51-90.
- GDPR. (2018). General data protection regulation. Retrieved November 21, 2020, from <https://gdpr-info.eu>

- Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, 42(4), 80-85.
- Jabar, A. A., & Ogunsola, A. (2022). Analytical review of e-commerce business models. *African Journal of Accounting and Financial Research*, 5(2), 48-60.
- Jumia Company Report. (2022). Retrieved from <https://group.jumia.com/news/jumia-technologies-is-the-best-of-amazon-in-africa>
- Kenya Data Protection Act. (2019). Retrieved from http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
- Kitukutha, N., & Oláh, J. (2018). Trust and e-commerce: Case study on Jumia company. *The Annals of the University of Oradea. Econ. Sci*, 27, 313-319.
- McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, 6(2), 35-59.
- Mwangi, E. W. (2021). Enhancing electronic government services in public organizations in Kenya: Case of Huduma Postal City Square in Nairobi (Doctoral dissertation, University of Nairobi).
- Okeke, R. I., Shah, M. H., & Ahmed, R. (2013). Issues of privacy and trust in e-commerce: Exploring customers' perspective. *Journal of Basic and Applied Scientific Research*, 3(3), 571-577.
- Olubusola, O., Mhlango, N. Z., Falaiye, T., Ajayi-Nifise, A. O., & Daraojimba, E. R. (2024). Digital transformation in business development: A comparative review of USA and Africa.
- Osita, G. C., Chisom, C. D., Okoronkwo, M. C., Esther, U. N., & Vanessa, N. C. (2022). Application of emerging technologies in mitigation of e-commerce security challenges. *CCU Journal of Science*, 2, 2734-3766.
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101-134.
- Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability, and consumer trust in electronic commerce transactions. *Logistics Information Management*, 15(5/6), 358-368.
- Ringel, G. (2022). E-commerce businesses: Five data privacy practices for gaining customer trust in 2022. *Journal of Business Research*.
- Saidu, M. A., Shamsudeen, L. S., Muhammad, A. K., & Abdulkadir, A. (2022). Exploring e-commerce opportunities for better international trading and tax revenue generation: A review for developing countries. *Journal of Science Technology and Education*, 10, 109-124.
- Schwandt, J. (1997). Electronic data interchange: An overview of its origins, status, and future. *Journal of Business Research*.
- Siau, K., & Shen, Z. (2003). Building customer trust in mobile commerce. *Communications of the ACM*, 46(4), 91-94.
- Soleimani, M. (2022). Buyers' trust and mistrust in e-commerce platforms: A synthesizing literature review. *Information Systems and E-Business Management*, 20, 57-78. <https://doi.org/10.1007/s10257-021-00545-0>
- Tidjani, C. (2021). COVID-19 and challenges of the Fintech industry: A state of the art and outlooks on the North African region. *Abaad Iktissadia Review*, 11, 696-721.
- Turban, E., Whiteside, J., King, D., & Outland, J. (2017). *Introduction to electronic commerce and social commerce*. Springer.
- Zaidan, M. N., & Raju, V. (2021). Literature review of factors affecting the online purchase intention in Iraq. *International Journal of Academic Research*, 7(7), 87-100.
- Zerbini, C., Bijmolt, T. H., Maestripieri, S., & Luceri, B. (2022). Drivers of consumer adoption of e-commerce: A meta-analysis. *International Journal of Research in Marketing*, 39(4), 1186-1208.

- Krawczyk, H. (2001, August). The order of encryption and authentication for protecting communications (or: How secure is SSL?). In Annual International Cryptology Conference (pp. 310-331). Berlin, Heidelberg: Springer.
- Broutsou, A., & Fitsilis, P. (2012, May). Online trust in the Greek context: The influence of perceived company's reputation on consumers' trust and the effects of trust on intention for online transactions. In Proceedings of the Management of International Business and Economic Systems (MIBES-ESDO) 2012 International Conference (pp. 1-10). School of Management and Economics, TEI of Larissa, Greece.
- Hils, M., Woods, D. W., & Böhme, R. (2020, October). Measuring the emergence of consent management on the web. In Proceedings of the ACM Internet Measurement Conference (pp. 317-332).
- Tian, W. (2022, December). E-commerce platform in the global south: Concepts, trends, and cases. In 2022 4th International Conference on Economic Management and Cultural Industry (ICEMCI 2022) (pp. 300-309). Atlantis Press.