INFORMATION SECURITY IN DIGITAL AGRO-TOURISM: CHALLENGES ASSOCIATED WITH IoT AND BIG DATA TECHNOLOGIES

CZU: 004.056:[338.48:004.738.5]
DOI: https://doi.org/10.53486/tids2026.30

SVETLANA CEBAN
ASEM, Chisinau, MD 2005, Republic of Moldova
e-mail: ceban.svetlana@ase.md
ORCID ID: 0009-0006-5957-7666

Abstract. This paper examines the main information security risks related to the use of Internet of Things (IoT) and Big Data technologies in agro-tourism. Digital technologies help agro-tourism businesses promote their services, communicate with customers and manage reservations. However, using online platforms and connected devices can also create security problems, especially when personal data is collected and stored.
The main aim of this study is to identify the security risks associated with these technologies and examine how agro-tourism businesses can manage them. The research is based on a review of scientific publications and institutional materials related to digital transformation, tourism and information security.
The analysis identifies several important issues, including unauthorized access to customer information, security weaknesses in connected devices, dependence on external service providers and limited staff awareness of cybersecurity risks. The study also presents possible measures that businesses can consider to protect information and use digital services more safely.
The findings suggest that information security requires attention not only to technology, but also to staff responsibilities and the management of digital services. Further research involving agro-tourism enterprises in the Republic of Moldova is needed to better understand how these risks are managed in practice.

Keywords: agro-tourism, digital transformation, information security, Internet of Things (IoT), big data, rural development

JEL Classification: L83, O33, Q16, M15

INTRODUCTION

Organizations engaged in tourism activities use online platforms to present their services, communicate with visitors and manage bookings. These platforms are particularly useful for agro-tourism businesses, as they allow potential visitors to plan their visits to rural tourism destinations remotely. Digital systems make an important contribution to the coordination of daily activities. However, each platform used or connected device raises questions about who has access to the information, how securely it is protected against unauthorized access, where it is stored and what level of protection is provided. These questions become more relevant when IoT devices and Big Data applications are introduced (Li *et al.*, 2018; OECD, 2020).

Information security is an important concern for small agro-tourism enterprises, where limited financial resources and the need for technical equipment may involve additional costs. Digital booking and payment platforms collect and store customers' personal data. Data protection is a major concern, and if data is not properly managed, agro-tourism organizations may face risks that could affect both their customers and their own activities. The scientific literature identifies this issue as a major risk requiring particular attention. However, the present study does not measure the frequency of such incidents.

Research on digitalization and digital transformation highlights major changes in organizational structures and management practices (Vial, 2019; Warner and Wäger, 2019). This perspective is

relevant to the agro-tourism sector, as the use of digital technologies also involves responsibilities related to personal data protection, system maintenance and the management of potential risks. In this context, the article raises the following question: What are the main information security challenges associated with the use of IoT and Big Data technologies in digital agro-tourism?

1. MATERIALS AND METHODS

This study analyzes published scientific research and institutional materials related to digital transformation, tourism, the Internet of Things (IoT), Big Data, and information security. The study relies on secondary sources of information, without conducting interviews, field observations, or original technical testing. Therefore, the analysis highlights the main categories of potential risks and the management measures used to address them, without estimating the frequency of incidents occurring in agro-tourism enterprises.

The analysis initially identifies the security issues presented in the selected publications. Subsequently, a comparative analysis identifies the differences between risks associated with connected devices, customer data processing, and the use of third-party platforms. In the final stage, the findings are synthesized into a structured framework that includes the identified risks, potential consequences, and relevant management measures to address them. The comparison is interpretive in nature, and no statistical meta-analysis was conducted.

The synthesis is organized around six main themes: personal data protection, unauthorized access, vulnerabilities of IoT devices, governance of systems that process large volumes of data, staff understanding of information security, and dependence on external service providers. These themes provide a practical framework for examining how technical and organizational decisions interact in the agro-tourism sector.

2. RESULTS AND DISCUSSION

The scientific literature examined indicates that security issues may arise at different stages of digital processes carried out within an agro-tourism enterprise. For example, making a reservation may involve the use of customers' personal data and an external platform, while a connected sensor may require an additional account or a new network connection.

The consequences are influenced by the systems used and the security measures implemented. Thus, the following analysis distinguishes between different types of risk exposure, without assuming that all digital technologies present the same type of risk.

Customer data management represents one of the areas exposed to security risks.

Reservation and payment processes may require the use of customers' names, contact details, and transaction information, some of which may be processed through external services. The main management aspects that need to be considered include data access, data retention periods, and the distribution of responsibilities between the enterprise and its service providers.

The literature on digital transformation provides a basis for examining these issues, although it does not, on its own, establish how widespread these problems are among agro-tourism enterprises in the Republic of Moldova (Vial, 2019).

Another important challenge is associated with IoT devices used in agro-tourism environments. Smart sensors, monitoring systems and connected devices are increasingly used for resource management, environmental monitoring and enhancing tourist experience. However, these devices are often vulnerable to cyberattacks due to weak authentication mechanisms, outdated software and

lack of security updates. These weaknesses may allow unauthorized access and create security problems for the systems used by the business.

Using external platforms can also create some challenges for agro-tourism businesses. For example, a business may use one platform for bookings and another for communication or data storage. These services make daily work easier because the business does not need to manage all the systems itself. However, it is still important to ensure that the services remain available, control who can access the information, and understand how customer data is used and protected.

Furthermore, insufficient cybersecurity awareness among staff and managers significantly increases the exposure to security threats. In many cases, employees are not trained to recognize phishing attacks, manage secure passwords or follow basic data protection practices. When employees are not familiar with basic security rules, mistakes may occur that put business information at risk. This review brings together the main technical and organizational risks, as well as those related to external service providers, in the context of agro-tourism. The study does not aim to measure the level of cybersecurity in rural businesses. Instead, it highlights the main issues that managers should consider when choosing and using digital services.

The main information security challenges identified in digital agro-tourism systems are summarized in Figure 1.



Figure 1. Information Security Challenges in Digital Agro-Tourism Systems.
Source: *Author's own elaboration.*

These findings show why agro-tourism businesses need to consider security when using digital technologies.

The main risks identified in the analysis can also be systematized according to the digital component involved, the possible impact on agro-tourism enterprises and the recommended security measures, as shown in Table 1.

Table 1. Main Information Security Challenges in Digital Agro-Tourism Enterprises.

Digital component	Main security risk	Possible impact	Recommended measure
IoT devices and sensors	Unauthorized access, weak authentication	System compromise, operational disruption	Strong authentication, regular updates
Online booking platforms	Exposure of customer and payment data	Data breaches, loss of customer trust	Secure storage, encryption, access control
Big Data systems	Misuse of personal and behavioral data	Privacy violations, reputational damage	Data governance and anonymization
Cloud services	Dependence on external providers	Service interruption, limited data control	Backup systems and provider assessment
Staff digital tools	Phishing, weak passwords, human error	Account compromise, financial and reputational risks	Cybersecurity training and password policies

Source: *Author's own elaboration based on Vial (2019), Gretzel et al. (2015) and Li et al. (2018).*

Table 1 presents the main digital technologies, their security risks, possible effects on business activities, and measures that can help reduce these risks. The table shows that different technologies need different security measures. For example, connected devices need regular updates and secure access, while customer data must be protected through clear rules on who can use and manage it. Staff training is also important for all these activities.

In the Republic of Moldova, this table can help agro-tourism businesses better understand the security risks related to digital technologies. Online advertising and booking platforms are useful for rural tourism, but this study does not provide direct information about how widely these services are used or how often cybersecurity incidents occur in Moldova. More research involving local agro-tourism businesses is needed to understand which risks are most important and how they can be managed in practice (World Tourism Organization, 2023; Biroul Național de Statistică, 2024; European Commission, 2021).

The use of digital technologies also raises questions about the long-term development of agro-tourism businesses. When these businesses depend on online platforms and digital systems, they need to consider how to protect customer information and keep their services working. Basic security measures can help reduce problems and maintain customer trust.

At the same time, digital security has become closely connected to the reputation and market position of agro-tourism enterprises. Tourists increasingly rely on online reservations, digital communication and electronic payments when choosing tourism services. Any cybersecurity incident involving personal data or online transactions may negatively affect customer confidence and reduce the competitiveness of rural tourism destinations. Therefore, information security should be integrated not only into technological management, but also into strategic planning and sustainable rural tourism development policies (Vial, 2019; OECD, 2020; UN Tourism, 2023).

3. PRACTICAL RECOMMENDATIONS FOR STRENGTHENING INFORMATION SECURITY IN DIGITAL AGRO-TOURISM

The risk categories discussed above highlight several management measures that agro-tourism enterprises can adapt to the systems they use. These are recommendations based on the review of scientific literature, rather than measures whose effectiveness was tested in the present study. The usefulness of these recommendations depends on the size of the enterprise, the services it uses, and the types of information it processes.

One important recommendation is that agro-tourism businesses should implement stronger access control measures, including secure password policies, multi-factor authentication and restricted access to sensitive data. These measures reduce the risk of unauthorized access to digital platforms, booking systems and internal databases.

Regular software updates and technical maintenance of IoT devices are also essential for preventing cyberattacks and reducing system vulnerabilities. Smart sensors and connected devices should be monitored continuously to ensure secure operation and timely detection of security incidents.

Customer information, booking records and payment data should also be protected through encryption and secure storage solutions. Data protection policies should comply with digital privacy standards and ensure the confidentiality and integrity of sensitive information.

Another important recommendation is the development of cybersecurity awareness among staff and managers. Employee training in recognizing phishing attempts, managing passwords securely and applying basic digital protection practices can significantly reduce human-related security risks.

Finally, agro-tourism enterprises should integrate cybersecurity into their broader digital transformation strategy. Information security should be approached not only as a technical issue, but also as a managerial and strategic component of sustainable business development.

These recommendations may help agro-tourism businesses protect customer information, reduce security risks and use digital services more safely (Vial, 2019; Gretzel et al., 2015; OECD, 2020).

The main practical measures that can be implemented by agro-tourism enterprises include the following:

- implementation of secure password policies;
- regular software and firmware updates for IoT devices;
- encryption of customer and payment data;
- employee cybersecurity awareness training;
- secure cloud data management;
- data backup and recovery planning;
- periodic cybersecurity risk assessment;
- compliance with cybersecurity and data protection regulations.

CONCLUSIONS

The literature review identifies several issues that require attention when IoT technologies, applications that process large amounts of data, and online services are used in agro-tourism. These include access to customer information, maintenance of connected devices, dependence on service providers, and staff practices. These issues are connected, but they require different security measures. The analysis provides a structured overview of possible risks without showing that a specific percentage of agro-tourism enterprises has experienced cyberattacks.

One of the main results of the study is the grouping of security issues according to digital components and the management measures needed. In this way, information security is not only a separate technical activity. It also requires decisions about the distribution of responsibilities, cooperation with service providers, and procedures followed by staff. This interpretation is consistent with the approaches presented in the literature on organizational digital transformation (Vial, 2019; Warner and Wäger, 2019).

The study is based on a qualitative analysis of secondary information sources and has certain limitations. The research did not include a representative sample of agro-tourism enterprises or actual data on cybersecurity incidents. In addition, no testing of IoT devices was carried out during the research. Future research could include interviews and surveys with owners of agro-tourism enterprises in the Republic of Moldova. This could help provide a clearer understanding of how digital technologies are used, what security measures are currently in place, and which of the proposed recommendations could be applied in practice.

The proposed framework can help organize future research on digital risks in rural tourism. Its importance lies in identifying the main factors that need to be examined in relation to data, devices, service providers, and staff practices. However, it should not be considered a validated model for evaluating cybersecurity performance.

For managers of agro-tourism enterprises and local stakeholders, the first step is to examine how digital services are used and to establish responsibilities for protecting the information they

process. Introducing basic security measures and reviewing relationships with service providers can contribute to safer and more stable business operations.

However, further research and analysis based on data collected directly from enterprises in the Republic of Moldova are needed to determine which of the proposed measures should be applied first and to evaluate their results.

REFERENCES

Biroul Național de Statistică, 2024. *Activitatea turistică a agenților de turism și turoperatorilor în anul 2023*. Available at: https://statistica.gov.md/ro/activitatea-turistica-a-agentiilor-de-turism-si-turoperatorilor-in-anul-2023-9491_60952.html [Accessed 10 January 2026]

European Commission, 2021. *Digital Transformation of Tourism*. Available at: https://ec.europa.eu [Accessed 10 January 2026].

Gretzel, U., Sigala, M., Xiang, Z. and Koo, C., 2015. Smart tourism: foundations and developments. *Electronic Markets*, 25(3), pp.179–188.

Li, L., Su, F., Zhang, W. and Mao, J.-Y., 2018. Digital transformation by SME entrepreneurs: A capability perspective. *Information Systems Journal*, 28(6), pp.1129–1157.

OECD, 2020. *Tourism Trends and Policies 2020*. Paris: OECD Publishing.

World Tourism Organization, 2023. Tourism and Rural Development: A Policy Perspective. Madrid: UNWTO. https://doi.org/10.18111/9789284424306.

Vial, G., 2019. Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), pp.118–144.

Warner, K.S.R. and Wäger, M., 2019. Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, 52(3), pp.326–349.