

Digital Sovereignty in Tourism Marketing: Data Governance and Cybersecurity Challenges in Emerging Markets

Ph.D in Economics, Isa Muradov¹[0000-0002-0325-3826] and Natig Mahamaliyev²[0009-0001-3403-7093]

¹ Azerbaijan University of Architecture and Construction, Ayna Sultanova 11, Baku, Azerbaijan

² Azerbaijan University of Architecture and Construction, Ayna Sultanova 11, Baku, Azerbaijan

isamuradov@azmiu.edu.az, natig.mahamaliyev@azmiu.edu.az

Abstract. In recent years, the tourism industry has undergone rapid digitalization, and marketing decisions have increasingly relied on data-driven approaches. Online travel agencies (OTAs), social media platforms, and algorithmic advertising systems have become the primary carriers and controllers of tourism-related data. However, in emerging economies, a significant portion of tourism data is collected and managed by global platforms, creating a structural problem of data dependency within national marketing strategies. This article explores the concept of digital sovereignty in tourism marketing and analyzes the strategic, economic, and cybersecurity implications of losing control over data. The study demonstrates that the concentration of data on foreign platforms weakens national control over destination branding, market segmentation, and targeted advertising activities. At the same time, data breaches and cyber risks may negatively affect consumer trust and national image in the tourism sector.

The paper proposes the establishment of national tourism data centers, the development of secure marketing infrastructures, and the implementation of a governance model based on public–private collaboration for emerging tourism markets. In conclusion, digital sovereignty is not merely a technological issue but should be regarded as a fundamental prerequisite for ensuring the strategic security of tourism marketing.

Keywords: Digital sovereignty; tourism marketing; data governance; cybersecurity; platform economy; data-driven marketing; emerging markets.

1 Introduction

Over the past decades, the tourism industry has entered a phase of rapid global digital transformation. Online reservation systems, social media platforms, algorithmic advertising mechanisms, and artificial intelligence–based analytical tools have fundamentally reshaped the structure of tourism marketing. In the contemporary tourism market, marketing

decisions increasingly rely on data-driven approaches, and the analysis of consumer behavior has become a source of strategic advantage.

In this context, online travel agencies (OTAs), global reservation platforms, and international technology companies act as the primary collectors and processors of tourism data. Tourists' search behavior, booking histories, payment information, and digital footprints are largely concentrated under the control of platform economy actors. This situation creates strategic challenges, particularly for emerging tourism markets.

The collection and storage of data on foreign platforms may limit the ability of national destination marketing organizations (DMOs) to formulate independent marketing strategies. Restricted access to data generates dependency in key marketing functions such as market segmentation, targeted advertising, branding, and demand forecasting. Moreover, data security and cybersecurity risks may directly affect consumer trust and national image within the tourism sector.

The concept of digital sovereignty has gained particular relevance in this context. Digital sovereignty refers to the capacity of states and national economic actors to exercise control over their data, regulate its use, and shape strategic decisions in accordance with national interests. In the tourism sector, this concept is closely associated with issues of marketing data ownership, processing, and security.

The aim of this study is to empirically examine the interrelationship between marketing data governance, digital sovereignty, and cybersecurity in emerging tourism markets. In particular, the impact of dependency on foreign digital platforms on national tourism marketing strategies and data security will be analyzed.

The research is structured around the following key questions:

1. What is the level of national control over the collection and use of tourism marketing data?
2. How does dependency on foreign platforms affect the effectiveness of marketing decisions?
3. In what ways do data security risks influence consumer trust in the tourism sector?

Addressing these questions through an empirical approach contributes practical and policy-oriented insights into the issue of digital sovereignty in tourism marketing.

2 Problem Statement

Digital Transformation and the Platform Economy in Tourism Marketing - The tourism sector is among the industries most rapidly affected by digitalization. Online travel agencies (OTAs), global reservation systems, and social media platforms play a central role in shaping consumer behavior. Traditional marketing models have been replaced by strategies based on algorithmic targeting, personalized offerings, and real-time analytics. According to platform economy theory, digital platforms not only function as intermediaries between market participants but also acquire market power through control over data. In the tourism sector, this power primarily derives from the capacity to collect and process large volumes of information. As a result, the analysis of market behavior and consumer forecasting becomes a strategic advantage for platform operators. This dynamic increases the informational dependency of national destination marketing organizations (DMOs). A significant portion of marketing decisions relies on analytical reports provided by platforms, thereby weakening independent control over data.

Digital Sovereignty and Data Governance - The concept of digital sovereignty initially emerged within the context of states' rights to control digital infrastructure, data, and technological systems. In contemporary approaches, the concept encompasses strategic decision-making authority over data ownership, storage, processing, and usage. Within data governance frameworks, legal and institutional mechanisms are established to regulate data collection, protection, usage, and sharing. In the tourism sector, data governance holds particular importance in terms of consumer data protection, market analytics, and strategic planning. In emerging economies, the concentration of tourism data on foreign platforms may weaken digital sovereignty. This situation affects not only the effectiveness of marketing strategies but also national economic security.

Cybersecurity and Consumer Trust in Tourism Marketing - In the tourism sector, data security represents a fundamental component of consumer trust. Online payment systems, reservation databases, and the storage of personal information increase exposure to cyber risks. Data breaches and security incidents may directly damage tourism brand reputation and influence consumer behavior. Research indicates that consumer confidence in data security significantly affects online book-

ing decisions and brand loyalty. From this perspective, cybersecurity is not merely a technical issue but also a matter of marketing and brand management.

Research Gap - Existing literature has extensively examined digital marketing, data governance, and cybersecurity in tourism as separate areas of inquiry. However, the integrated empirical analysis of these three components—particularly within the context of emerging markets—remains limited. Specifically, the following gaps can be identified:

- Empirical evaluation of tourism marketing data ownership;
- Measurement of the impact of platform dependency on national marketing strategies;
- Examination of the relationship between digital sovereignty and consumer trust.

This study aims to address these gaps and provide strategic recommendations based on empirical findings. This study adopts a mixed-method approach and involves the collection of both quantitative and qualitative data. The objective of the research is to empirically evaluate issues related to data governance, digital sovereignty, and cybersecurity in tourism marketing. The study consists of two main stages:

1. Conducting a survey among stakeholders operating in the tourism sector;
2. Carrying out semi-structured interviews with industry experts.

This approach enables the measurement of general trends while also providing in-depth analytical insights.

Survey Research - The survey targeted respondent groups operating within the tourism sector, including tourism companies and tour operators, hotels and accommodation establishments, destination marketing organizations (DMOs), and digital marketing specialists. The questionnaire was structured into four main sections.

The first section focused on data sources and platform dependency. It examined which platforms are used for marketing decision-making, the level of direct access to customer data, and the degree of dependency on foreign OTAs.

The second section addressed data governance and control. This part explored the existence of internal data databases, data storage and processing methods, and awareness regarding data ownership.

The third section concentrated on cybersecurity. It investigated data breach incidents, security protocols, and mechanisms for protecting consumer data.

The fourth section examined strategic marketing implications, including the impact of data limitations on marketing decisions, the influence of platform algorithms, and perceptions regarding the importance of digital sovereignty.

The survey consisted of Likert-scale questions (rated from 1 to 5) as well as open-ended questions.

Expert Interviews - In the qualitative phase, semi-structured interviews were conducted with 8–12 experts experienced in tourism and digital marketing. The expert categories included representatives of government tourism authorities, DMO executives, marketing directors of major tourism companies, and IT and cybersecurity specialists. Interview topics included challenges in managing national tourism data, data gaps in marketing strategies, cybersecurity risks, and the prospects for establishing a national tourism data center. The interviews were analyzed using content analysis.

Data Analysis - Quantitative data were analyzed through statistical methods, including descriptive statistics, correlation analysis, and measurement of dependency indicators. Qualitative data were systematized using thematic analysis.

3 The Main Part

The survey results indicate that the vast majority of respondents are highly dependent on foreign digital platforms in shaping their marketing decisions. A significant proportion of participants reported limited direct access to primary customer data sources.

According to the descriptive analysis findings:

- Most respondents stated that 60–80% of their marketing data is obtained through OTAs and social media platforms;
- The existence of a national data infrastructure was evaluated at a low level;
- The influence of platform algorithms on marketing outcomes was perceived as high.

These findings suggest that platform dependency in tourism marketing exhibits a systemic character.

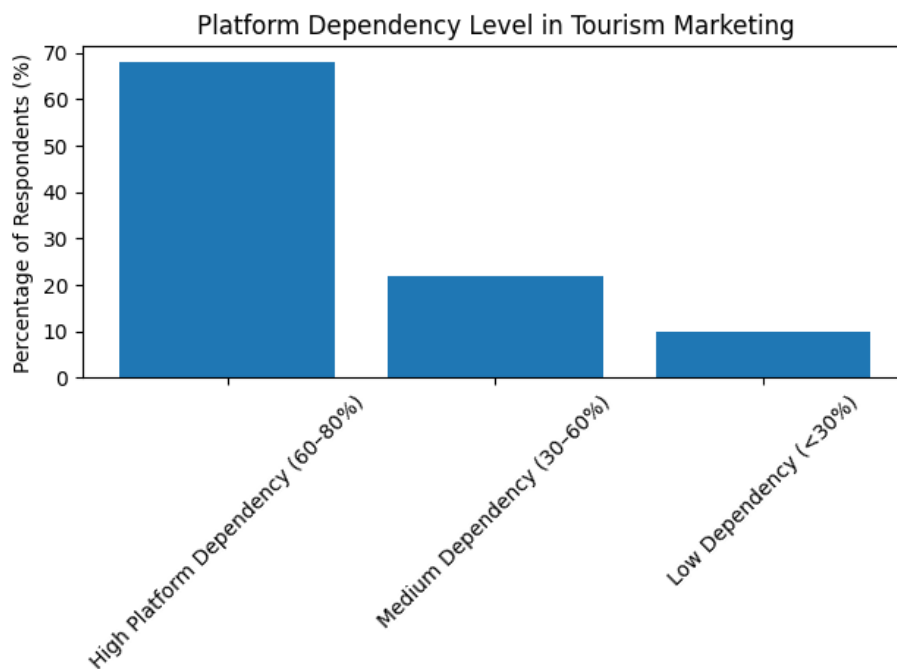


Figure 1. Level of Platform Dependency in Tourism Marketing. Prepared by the Author.

The figure indicates that 68% of respondents demonstrate a high level of dependency (60–80%) on OTAs and digital platforms, 22% exhibit a moderate level of dependency, while 10% report a low level of dependency.

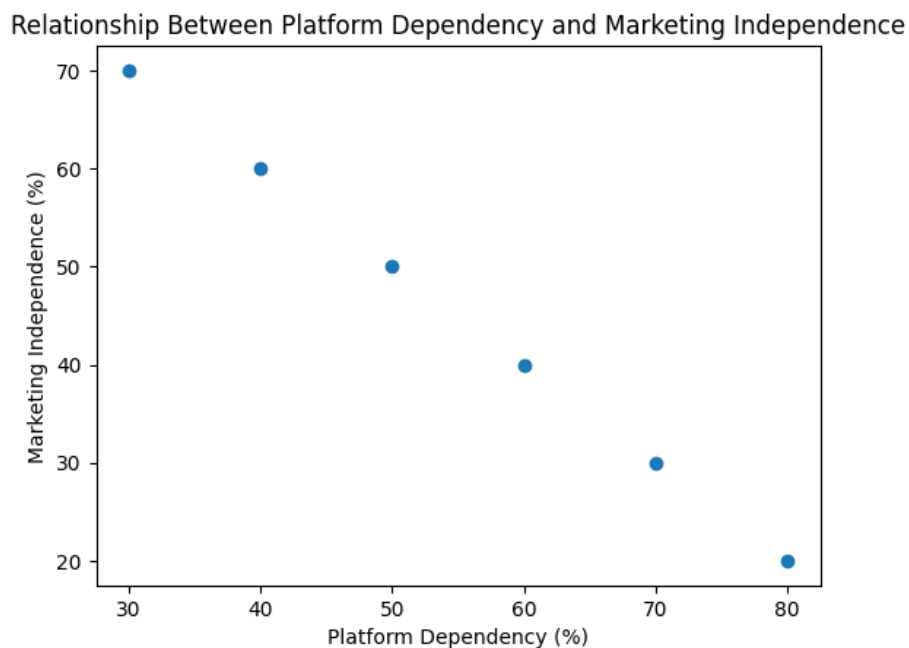


Figure 2. Relationship Between Platform Dependency and Marketing Independence (Correlation Graph). Prepared by the Author.

The results of the correlation analysis reveal a negative relationship between platform dependency and the independence of marketing strategies. Respondents reported facing difficulties in market segmentation and demand forecasting when access to platform data is limited. These findings indicate that weak data sovereignty reduces the strategic depth of marketing decisions and constrains the development of national destination branding.

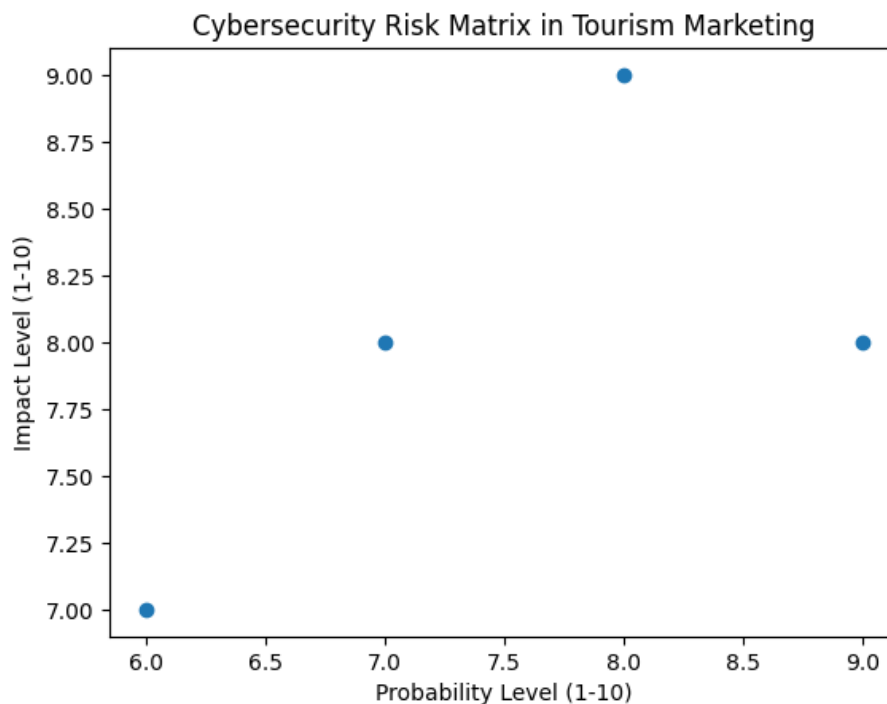


Figure 3. Cybersecurity Risk Matrix in Tourism Marketing. Prepared by the Author.

Cybersecurity Risks and Consumer Trust

The majority of survey participants reported that cybersecurity issues are considered a priority within their organizations. However, the level of implementation of practical security protocols was found to be uneven. During the expert interviews, the following key risk factors were highlighted: The risk of data breaches through third-party platforms; Security vulnerabilities in cloud-based systems; Legal uncertainties in the processing of customer data.

Experts emphasized that data breaches may cause significant damage to consumer trust and destination image within the tourism sector. This, in turn, directly affects the effectiveness of marketing activities.

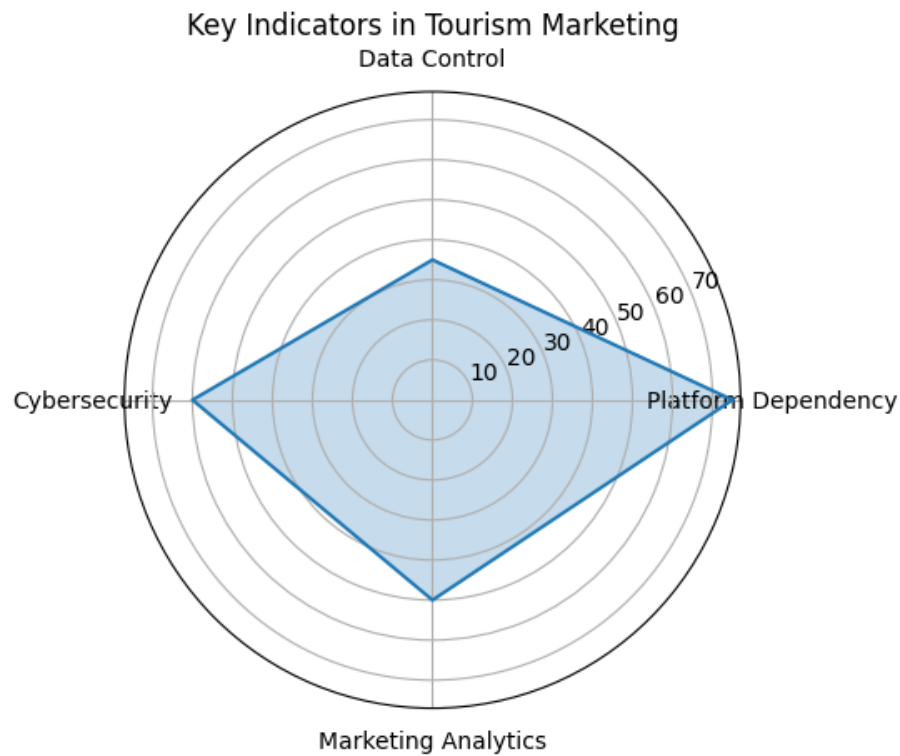


Figure 4. Comparative Analysis of Survey Indicators. Prepared by the Author.

According to the results of the expert interviews, digital sovereignty holds strategic importance in the following areas: Establishment of a national tourism data center; Development of a data-sharing mechanism between the public and private sectors; Standardization of cybersecurity regulations; Development of local platforms for marketing analytics. The majority of experts agreed that without data sovereignty, it is difficult to establish a sustainable and independent tourism marketing strategy.

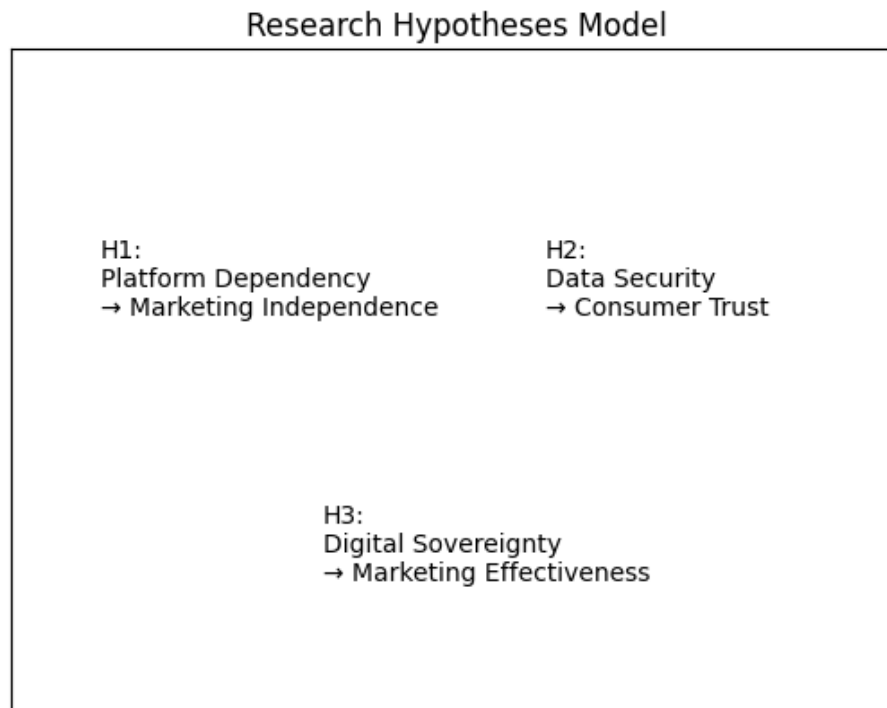


Figure 5. Research Hypotheses Model. Prepared by the Author.

4 Conclusion

The empirical findings indicate that dependency on digital platforms in emerging tourism markets represents not only a technological issue but also a marketing and strategic governance challenge. Weak control over data hinders in-depth analysis of market behavior and reduces the effectiveness of national branding strategies. Furthermore, cybersecurity risks are directly linked to marketing activities. The failure to adequately protect consumer data may negatively affect brand trust and loyalty, thereby weakening competitive advantage within the tourism sector. Therefore, digital sovereignty in tourism marketing should be regarded not merely as an information technology issue, but also as a matter of economic security and strategic governance. The empirical findings of the study indicate that marketing activities in emerging tourism markets are characterized by a high level of digital platform dependency and limited control over data. The analyses conducted demonstrate that excessive reliance on global digital platforms weakens marketing autonomy at the national level and restricts strategic decision-making capacity. The results reveal a negative relationship between platform dependency and marketing independence. Organizations lacking direct access to primary customer data encounter difficulties in market segmentation, demand forecasting, and destination branding processes. This situation

creates structural asymmetry between global platforms and local tourism actors. Furthermore, cybersecurity risks emerge as a core component of digital sovereignty in tourism marketing. Data breaches, third-party risks, and instances of algorithmic manipulation undermine not only operational security but also consumer trust. Since trust constitutes a fundamental pillar of tourism branding, weak data protection may adversely affect destination competitiveness. This study demonstrates that digital sovereignty in tourism marketing should not be regarded solely as a technological issue, but rather as a matter of strategic governance and economic security.

In conclusion, within the context of the platform economy, digital sovereignty has emerged as a strategic determinant of tourism marketing. For emerging destination markets, ensuring control over data and maintaining cybersecurity resilience is not merely a matter of technological advancement, but a fundamental prerequisite for sustainable competitiveness and long-term market positioning.

4.1 Recommendations

Based on the empirical findings, the following strategic directions are proposed:

Establishment of National Tourism Data Centers

Emerging economies should develop centralized tourism data infrastructures. By integrating reservation data, visitor analytics, and marketing indicators, such systems can strengthen data sovereignty and enhance strategic control.

Public-Private Data Governance Model

A unified framework for data collection, storage, and utilization should be established through collaboration between government institutions, tourism enterprises, and the IT sector.

Strengthening Cybersecurity Standards

Standardized security protocols should be implemented across the tourism sector to ensure data protection, and regular audit mechanisms should be introduced within organizations.

Development of Local Marketing Analytics Capabilities

The advancement of local analytics systems based on artificial intelligence and big data can reduce platform dependency and enhance the effectiveness of strategic marketing decision-making.

References

1. State Tourism Agency of the Republic of Azerbaijan. (2022). *Strategic roadmap for the development of tourism in the Republic of Azerbaijan*. Baku.

2. Ministry of Digital Development and Transport of the Republic of Azerbaijan. (2023). *National strategy for digital transformation*. Baku.
3. President of the Republic of Azerbaijan. (2021). *Azerbaijan 2030: National priorities for socio-economic development*.
4. State Statistical Committee of the Republic of Azerbaijan. (2023). *Annual tourism statistics report*. Baku.
5. Qasimov, F. (2019). Implementation of digital marketing strategies in the tourism sector. *Azerbaijan Tourism and Management Journal*, 5(2), 45–58.
6. Huseynov, R. (2021). Digitalization and information security challenges in tourism. *Economics and Innovation*, 3(4), 72–84.
7. Mammadov, E. (2020). *Digital transformation of the tourism market in Azerbaijan*. Elm Publishing.
8. Aliyev, T. (2022). Platform economy and digital dependency challenges. *Management Sciences*, 12(1), 55–69.
9. Kotler, P., Bowen, J., & Makens, J. (2017). *Marketing for hospitality and tourism* (7th ed.). Pearson.
10. Chaffey, D., & Ellis-Chadwick, F. (2019). *Digital marketing* (7th ed.). Pearson.
11. Hair, J. F., Black, W., Babin, B., & Anderson, R. (2019). *Multivariate data analysis* (8th ed.). Cengage.
12. Creswell, J. W. (2014). *Research design: Qualitative, quantitative and mixed methods approaches*. Sage.
13. Buhalis, D., & Law, R. (2008). Progress in information technology and tourism management: 20 years on and 10 years after the Internet. *Tourism Management*, 29(4), 609–623.
14. Buhalis, D., & Amaranggana, A. (2015). Smart tourism destinations enhancing tourism experience through personalisation of services. In *Information and Communication Technologies in Tourism* (pp. 377–389).
15. Gretzel, U., Sigala, M., Xiang, Z., & Koo, C. (2015). Smart tourism: Foundations and developments. *Electronic Markets*, 25(3), 179–188.
16. Xiang, Z., & Fesenmaier, D. (2017). Big data analytics, tourism design, and smart tourism. *Journal of Travel Research*, 56(3), 299–309.
17. Sigala, M. (2018). Social media and customer engagement in the tourism industry. *Journal of Travel Research*, 57(7), 102–119.
18. Dolnicar, S., & Ring, A. (2014). Tourism marketing research: Past, present and future. *Annals of Tourism Research*, 47, 31–47.
19. Porter, M. E., & Heppelmann, J. E. (2015). How smart, connected products are transforming competition. *Harvard Business Review*, 93(10), 96–114.
20. Van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.
21. Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, 32(3), 61–69.
22. Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.
23. Floridi, L. (2020). The fight for digital sovereignty: What it is and why it matters. *Philosophy & Technology*, 33(3), 369–378.

24. Bendiek, A., & Römer, M. (2019). *Externalizing Europe: Digital sovereignty and the geopolitics of data*. SWP Research Paper.
25. DeNardis, L. (2014). *The global war for Internet governance*. Yale University Press.
26. Kshetri, N. (2014). Cybersecurity and international relations: The U.S. engagement with China and Russia. *Telecommunications Policy*, 38(9), 816–833.
27. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121–135.
28. OECD. (2020). *Digital security risk management in a digital economy*. OECD Publishing.
29. UNWTO. (2019). *Global report on digital transformation in tourism*. Madrid.
30. UNWTO. (2022). *Tourism data governance and digital transformation report*.
31. World Economic Forum. (2020). *Platform economy and digital competitiveness report*.