

Article

Digital privacy in tourism management: An interdisciplinary analysis of trends, challenges, and solutions

Emeka Austin Ndaguba^{1,*}, Cina van Zyl¹¹ Department of Applied Management, College of Economic and Management Sciences, University of South Africa, Pretoria 0003, South Africa* Corresponding author: Emeka Austin Ndaguba, emeka@ndaguba.net**CITATION**

Ndaguba EA. (2025). Digital privacy in tourism management: An interdisciplinary analysis of trends, challenges, and solutions. *Journal of Infrastructure, Policy and Development*. 9(4): 9131.
<https://doi.org/10.24294/jipd9131>

ARTICLE INFO

Received: 14 September 2024
Accepted: 8 October 2024
Available online: 21 November 2025

COPYRIGHT

Copyright © 2025 by author(s).
Journal of Infrastructure, Policy and Development is published by EnPress Publisher, LLC. This work is licensed under the Creative Commons Attribution (CC BY) license.
<https://creativecommons.org/licenses/by/4.0/>

Abstract: The widespread adoption of digital technologies in tourism has transformed the data privacy landscape, necessitating stronger safeguards. This study examines the evolving research environment in digital privacy in tourism management, focusing on publication trends, collaborative networks, and social contract theory. A mixed-methods approach was employed, combining bibliometric analysis, social contract theory, and qualitative content analysis. Data from 2004 to 2023 were analyzed using network visualization tools to identify key researchers and trends. Findings from the study highlights a significant increase in academic attention after 2015, reflecting the industry's growing recognition of digital privacy. Social contract theory provided a framework emphasizing transparency, consent, and accountability. The study's contribution towards literature are expansive, it is among the first study;s to expand the notion of social contract theory in digital privacy in tourism management. Furthermore, a core contribution of the study is its focus on how transparency, consent, and accountability are central to digital privacy management. Both the findings and contributions hold practical technological solutions to privacy challenges, by exploring actionable recommendations for tourism organizations to implement stronger data security protocols. It showcases how emerging technologies can offer novel methods of enhancing data protection, transparency, and user empowerment in the tourism industry.

Keywords: digital privacy; tourism management; social contract theory; data protection; interdisciplinary research; emerging technologies

1. Introduction

The widespread adoption of digital technology in the field of international tourism has significantly transformed the manner in which people traverse and encounter the world, while also redefining the dynamics of trust and accountability between visitors and organizations (Adekuajo et al., 2023; Collado-Agudo, Herrero-Crespo & San Martín-Gutiérrez, 2023). This transition is consistent with the conclusions given by Buhalis and Amaranggana (2015), who highlight the profound influence of digital technology on the tourism industry. Asserting the significance of transparency, consent, and accountability in data practices, social contract theory provides valuable insights into the implicit agreement governing the protection of tourists' digital privacy rights. The recent research conducted by Bec, Moyle, Schaffer & Timms, K. (2021). emphasizes the growing dependence on mobile technology and virtual reality, and considers it a second chance for virtualization to grow. Furthermore, Pencarelli (2020) investigate the function of artificial intelligence in augmenting customized travel experiences while simultaneously tackling privacy issues.

Through an analysis of the convergence of digital technologies, tourism practices, and social contract theory, this research seeks to reveal important obstacles and possibilities in protecting the digital privacy rights of tourists and provide practical suggestions for improving privacy measures in the era of digital tourism. Privacy is not only a convenience, but rather a basic human entitlement necessary for personal independence and dignity, as argued by Cavusoglu, Mishra, and Raghunathan (2015), who analyze the influence of strong privacy protections on user confidence. Moreover, Bieker (2022) examine the legal structures that support data protection in different countries, emphasizing the most effective methods for international tourism practitioners (Schwartz, 1994; Phillips, 2018).

Given the nature of international tourism, where personal information such as passport information, trip plans, and financial data are regularly exchanged, safeguarding privacy becomes of utmost importance (Shah, Jhanjhi & Brohi, 2024; Babin & Harris, 2023). The implementation of comprehensive data protection rules and regulations by governments and organizations is imperative to guarantee transparency in data collecting procedures and to secure explicit agreement from tourists for the utilization of their personal information. These ideas are further supported by the concepts of social contract theory, in which explicit permission serves as the foundation for trust and mutual agreement. Through the provision of data control to individuals, we strengthen the fundamental concept of privacy as an inherent entitlement of every human being, aligning with the viewpoint articulated by Puhretmair, Adamer, and Schmoelz (2018) on the necessity of implementing complete privacy measures.

According to Tyan et al. (2021), the incorporation of blockchain technology in data management offers novel approaches to improve data security and provide greater transparency. The right to security of person also applies to the digital domain, requiring the implementation of measures to safeguard individuals against damage caused by data breaches and unauthorised entry to personal information. Tourism industry organisations are obligated to adopt rigorous data security protocols, such as encryption, firewalls, and intrusion detection systems, as recommended by Tenopir and King (2000) in their analysis of the significance of data security in promoting trust. It is imperative to have timely and efficient reaction procedures to handle data breaches, therefore minimizing damage to impacted tourists and maintaining their entitlement to security. By giving foremost importance to the protection of visitors' data, we assert the notion that human rights go beyond physical limitations and encompass the digital realm, therefore guaranteeing the preservation of trust in digital platforms.

Notwithstanding the growing recognition of digital privacy concerns in the context of international travel, there is a significant deficiency in academic investigation. A notable dearth of extensive research exists that thoroughly examines the complex interaction between digital technology, tourism practices, and social contract theory in protecting the rights of tourists. Insufficient knowledge in this area impedes our capacity to understand the intricate difficulties and possible advantages arising from the digitalization of global tourism, especially with digital privacy. Recent scholarly works highlight the necessity of conducting further empirical studies to formulate efficient approaches that harmonize technology progress with the crucial

task of safeguarding the privacy rights of visitors (Ndaguba and Arukwe, 2024). Furthermore, it is essential to comprehend many stakeholder viewpoints, including those of travelers, tourism organizations, government agencies, and privacy advocates, in order to create comprehensive strategies for safeguarding digital privacy (Lee & Chen, 2021). Lacking thorough empirical research, it is difficult to detect deficiencies in current practices and develop methods to improve the safeguarding of visitors' digital privacy rights while simultaneously fostering innovation and expansion in the tourism sector. The research on digital privacy in tourism management reveals several significant gaps that need to be addressed. While regulations like GDPR have been studied extensively in general contexts (Voigt & Von dem Bussche, 2017), their specific application within tourism remains underexplored. Emerging technologies such as blockchain and AI have been proposed as solutions for privacy challenges (Zheng et al., 2018; Pencarelli, 2020), but empirical studies on their practical adoption in tourism are scarce. Additionally, interdisciplinary research integrating technology, law, and tourism management is limited, despite scholars like Gong & Schroeder (2022) and Li et al. (2023) addressing individual components. Existing literature also largely overlooks tourists' perspectives on privacy issues, focusing more on organizational practices (Yallop & Wilson, 2023). Furthermore, while social contract theory has been applied in other industries, its use in understanding privacy practices in tourism is minimal (Tussyadiah, Koo, & Jung, 2017). While, a global perspective on harmonizing privacy regulations across regions is lacking, leaving tourism organizations navigating fragmented regulatory environments (Greenleaf, 2014; Johnson & Verdicchio, 2023). Addressing these gaps will provide a more comprehensive understanding of digital privacy in tourism.

In an interconnected global society, the improper use of personal data might sustain discriminatory actions, specifically aimed at persons on the basis of characteristics such as nationality, race, or socioeconomic standing. In order to maintain the concept of freedom from discrimination, organizations must guarantee just and impartial treatment when collecting and using the personal data of tourists. Vulnerable groups, such as refugees or minority communities, should receive particular consideration as their data may be more susceptible to misuse. Chen, Wu & Wang, (2023) emphasizes the need for AI fairness and inclusivity in data methods to guarantee that it eliminates discrimination. Furthermore, Yallop et al.,(2023) analyze the ethical consequences of data analytics in the tourism industry and propose the implementation of regulations that prohibit the use of biased data. The establishment of an atmosphere characterized by inclusiveness and absence of prejudice serves to reinforce the universal nature of human rights within the realm of international tourism.

The advancement of digital technology in the field of international tourism brings up both advantageous prospects and obstacles in safeguarding human rights. Our adoption of a human rights viewpoint emphasizes the fundamental importance of privacy, security, and freedom from discrimination in the era of digital technology. Effective collaboration among governments, organizations, and stakeholders is necessary to establish strong legal frameworks, enforce rigorous security measures, and foster openness and accountability in data practices (Gong & Schroeder, 2022). Only by implementing coordinated measures to preserve digital privacy can we guarantee that international travelers can confidently explore the world, with the

assurance that their basic rights are upheld and safeguarded. The present study contributes to the current social contract theory by expanding its relevance to the digital domain, therefore illustrating how its concepts might direct the establishment of equitable and efficient data privacy measures within the tourism sector. This paper focuses on how the concepts of social contract theory might direct the establishment of strong digital privacy measures in the tourism sector, therefore guaranteeing trust and collaboration between visitors and organizations in the era of digitalization.

2. Theoretical framework

Social contract theory, originating from the works of philosophers such as Thomas Hobbes, John Locke, and Jean-Jacques Rousseau, provides a theoretical framework to understand the relationship between individuals and the institutions that govern them (Gustafsson, 2023). In the context of safeguarding digital privacy and human rights in international tourism, the principles of social contract theory can elucidate the implicit agreement between tourists and organizations regarding the protection of personal data (Chirieleison & Rizzi, 2023; Rousseau, 1762; Locke, 1690; Hobbes, 1651).

According to social contract theory, individuals in a society implicitly agree to abide by certain rules and norms in exchange for the benefits and protection provided by governing institutions. In international tourism, tourists entrust their personal information to various organizations involved in travel arrangements, expecting a level of protection and respect for their privacy in return (Lee, 2024). Recent literature, such as that by Tussyadiah, Koo, and Jung (2017), highlights the growing reliance on mobile technologies, necessitating stringent data protection practices to maintain this trust. Similarly, Buhalis and Amaranggana (2015) emphasize the transformative impact of digital technologies on tourism, underscoring the need for robust privacy measures to safeguard user data.

This study underscores the importance of transparency, consent, and accountability in data practices, reflecting the principles of a social contract between tourists and organizations (Yıldırım, 2021; Ortega-Rodríguez, C., Licerán-Gutiérrez, A., & Moreno-Albarracín, 2020; Sandbrook et al., 2021). Tourists willingly provide their personal data for travel arrangements, accommodation bookings, and other services, expecting organizations to handle this information responsibly and in accordance with established norms and regulations (Tassikas, 2021; Härkönen, 2020). Explicit consent from tourists for the collection and use of their personal data aligns with the idea of a social contract, where trust and mutual agreement form the basis of the relationship between individuals and organizations (Pencarelli, 2020).

Moreover, the emphasis on fairness and non-discrimination in data practices is crucial. Ensuring equal treatment for all tourists, regardless of nationality, ethnicity, or other characteristics, resonates with social contract theory, which posits that individuals agree to abide by rules that promote the common good and ensure equal treatment under the law (Yallop et al., 2023). Scholars like Puhretmair, Adammer, and Schmoelz (2018) highlight the importance of integrating diverse perspectives to develop comprehensive privacy solutions that protect all users equitably.

The right to security of person extends to the digital realm, necessitating measures to protect individuals from harm resulting from data breaches and unauthorized access to personal information (Pangrazio & Sefton-Green, 2021; DeNardis, 2020; Pohle & Thiel, 2020). Organizations operating in the tourism sector bear a responsibility to implement stringent data security measures, including encryption, firewalls, and intrusion detection systems (Tyan et al., 2021). Prompt and effective response protocols must be established to address data breaches, mitigating harm to affected tourists and upholding their right to security. In prioritizing the security of tourists' data, we affirm the principle that human rights transcend physical boundaries and extend into the digital sphere (Gong, & Schroeder, 2022).

Social contract theory provides a theoretical lens to understand the implicit agreement between tourists and organizations regarding personal data protection in international tourism. By upholding principles of transparency, consent, fairness, and accountability, organizations can honor this social contract and foster trust and cooperation with tourists, thereby safeguarding their digital privacy and human rights. This study adds to the existing theory by extending its application to the digital realm, demonstrating how its principles can guide the development of fair and effective data privacy practices in the tourism industry. Hence, this study aims to analyze the challenges and opportunities in safeguarding tourists' digital privacy rights and propose actionable recommendations for enhancing privacy measures in the digital age of tourism.

3. Materials and Methods

Data collection strategy

This research utilised Dimensions AI to collect data for analysing the challenges and opportunities in safeguarding tourists' digital privacy rights and propose actionable recommendations for enhancing privacy measures in the digital age of tourism. Dimensions AI accelerates research discovery in several ways. Firstly, it provides access to the world's largest collection of interconnected global research data, ensuring that researchers have access to a comprehensive and diverse range of information. This extensive database is accessible via a user-friendly web platform, allowing researchers to quickly search for and access relevant research data.

Secondly, Dimensions AI offers a suite of time-saving solutions and workflow-based applications that streamline the research process (Ndaguba and Marais, 2023). These solutions help researchers connect the dots across the research ecosystem, making it easier to identify new technologies, spot research opportunities, and stay ahead of competitors. With visual and interactive applications, researchers can analyse millions of research outputs in seconds, enabling them to conduct horizon scanning and complex landscape analysis with ease.

Additionally, Dimensions provides custom solutions tailored to the specific needs of organizations (Ndaguba et al., 2022). Their team of expert data scientists can create customized solutions to solve research questions and uncover precise information needed for decision-making. By leveraging these solutions, researchers and organizations can drive efficiencies in their workflow, saving valuable time and resources (Ndaguba, Brown, Marinova & Jogulu, 2024). While Dimensions AI is

critical for gaining access, PRISMA is the logic or model for ensuring transparency of entries for repetition.

PRISMA Model

The PRISMA model, which stands for Preferred Reporting Items for Systematic Reviews and Meta-Analyses, is a widely recognized framework used in research to ensure transparency and rigor in the reporting of systematic reviews and meta-analyses. The PRISMA model provides a structured approach for conducting literature searches, screening articles for relevance, and including eligible studies in the final analysis (see **Figure 1**).

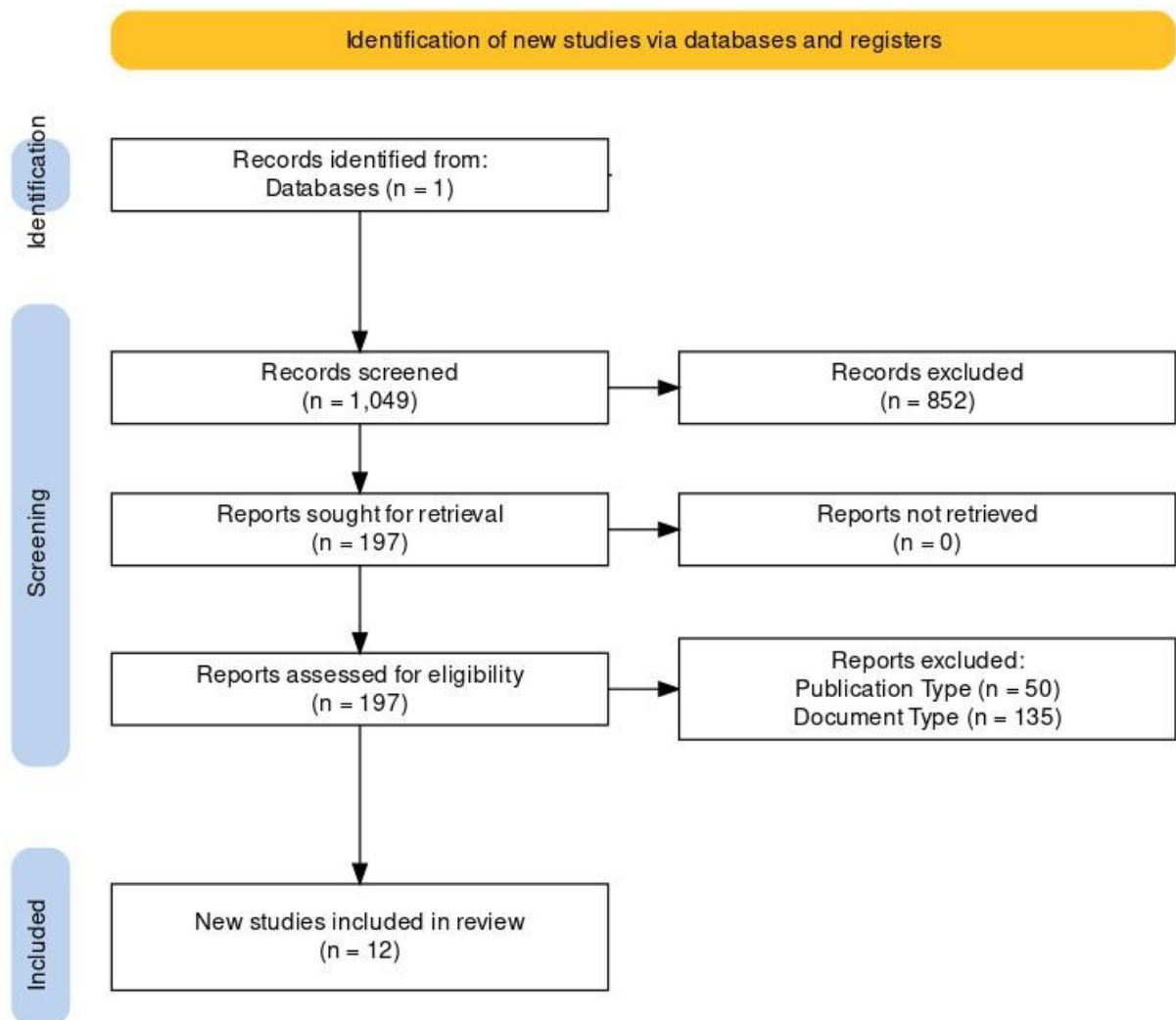


Figure 1. PRISMA model for tourists' digital privacy rights.

The PRISMA model typically consists of three main stages or layers:

- Identifying: In this stage, the researchers search the database of Dimensions AI for relevant studies using predefined search terms and criteria. The Boolean query for the research was:

("digital privacy" OR "privacy rights" OR "data protection") AND ("international tourism" OR "tourism industry") AND ("social contract theory" OR "human rights perspective") AND ("challenges" OR "opportunities" OR "gaps" OR "research questions").

This query captures the key concepts and themes discussed in the paper, including digital privacy, international tourism, social contract theory, human rights perspective, challenges, opportunities, gaps, and research questions. By combining relevant keywords with Boolean operators (such as AND, and OR), the query helps to refine search results and identify sources that address the specific focus of the conversation. The goal is to identify all relevant studies that meet the inclusion criteria for the review.

- **Screening:** after the completion of the initial search, the researchers screen the retrieved studies to determine their relevance and fitness to the research question. This involves reviewing titles and abstracts to identify potentially eligible studies and excluding those that clearly do not meet the inclusion criteria. However, before that it must be stated that the initial search generated 1,049 publications, including book chapter, edited books, newspapers among others. The next action was to stream the number of years to be assessed, and the researchers went with 2004-2023, which is two-decade worth of research. The essence was to capture effectively, the years when the issues of privacy and data breaches became more prevalent. The data was left with 1,049 demonstrating our argument that before 2004, there were fewer discuss on this research. Hence, this research is both new and contemporary, as issues of privacy, data breaches and its impact on international tourist users are still unfolding and the true cost unattained.

Limiting the study within the tourism sector and related field, three key fields of research emerge from ANZSRC 2020: Commerce, Management, Tourism and Services; Human Society; History, Heritage and Archaeology; Information and Computing Sciences; Law and Legal Studies; and Philosophy and Religious Studies of the ANZSRC 2020. Hence, the data plummeted further from 1,040 to 197 publications. Furthermore, when the 197 publications were further subjected to pruning regarding publication types (edited books, article, book chapter) and document types (reference works, article, review article, and review), 12 publications were left. Thus, the full-text articles of potentially relevant studies were then assessed against the inclusion criteria to determine the final eligibility for inclusion in the review, and only 11 of the publication fit the criteria and was included for data analysis, which were then subjected to final analysis.

- **Including:** In this final stage, researchers include eligible studies in the systematic review or meta-analysis based on predetermined criteria. This may involve extracting data from included studies, assessing the quality of the evidence, and synthesizing the findings to address the research question or objectives of the review.

By following the PRISMA model, researchers ensure that their systematic reviews and meta-analyses are conducted in a transparent, reproducible, and methodologically rigorous manner. Adhering to the PRISMA guidelines enhances the credibility and reliability of the research findings and facilitates comparison and interpretation of results across studies.

Data analysis

Data for this research is analysed using VOSviewer. VOSviewer is a software tool used for visualizing and analyzing bibliometric networks. It is commonly employed in academic research to explore patterns and relationships within large sets of scholarly literature. VOSviewer offers several key functionalities:

- **Visualization of Bibliometric Networks:** VOSviewer allows users to create visual representations of bibliometric networks, such as number of publications published in each year (see **Figure 2**), co-authorship networks (**Figure 3**), research organisation co-author citation networks (**Figure 4**), while journal citation (**Table 1**) and publisher citation (**Table 2**) can be found in tables. These networks and tables are typically represented as nodes (e.g., authors, papers, keywords) connected by edges (e.g., co-authorship, citation relationships).

- **Clustering and Mapping:** VOSviewer employs clustering algorithms to identify groups or clusters of related nodes within bibliometric networks. These clusters can represent thematic areas, research communities, or disciplinary subfields. The next section would provide, how the data gathered through the three step processes are transformed into visualization for ease of communication and presentation, demonstrating trends and linkages between variables, scholars, institutions, and nations.

4. Results

The provided visualizations and data reveal significant trends and patterns in the publication landscape concerning digital privacy within tourism management. These insights, when juxtaposed with existing literature, paint a comprehensive picture of the evolving academic discourse in this field.

The trend in publications from 2004 to 2023 (**Figure 2**) demonstrates a notable surge in scholarly output, particularly from 2015 onward. This increase aligns with broader academic and industry recognition of the critical intersection between digital privacy and tourism management. The year 2022 stands out with five publications, the highest in the observed period, followed closely by four in 2021 and three in 2023.

Network visualizations of co-authors (**Figure 2**) and institutions (**Figure 3**) further elucidate the collaborative nature of research in this domain. Prominent clusters of authors, such as those including Hermes, Sebastian, Clemons, Eric K., and Waran, Ravi V., suggest active collaborative networks driving research innovation. These clusters indicate that research on digital privacy in tourism management benefits from diverse, interdisciplinary contributions, fostering robust academic discourse. Notably, some authors and institutions appear more isolated, indicating areas where increased collaboration could further enhance research impact.

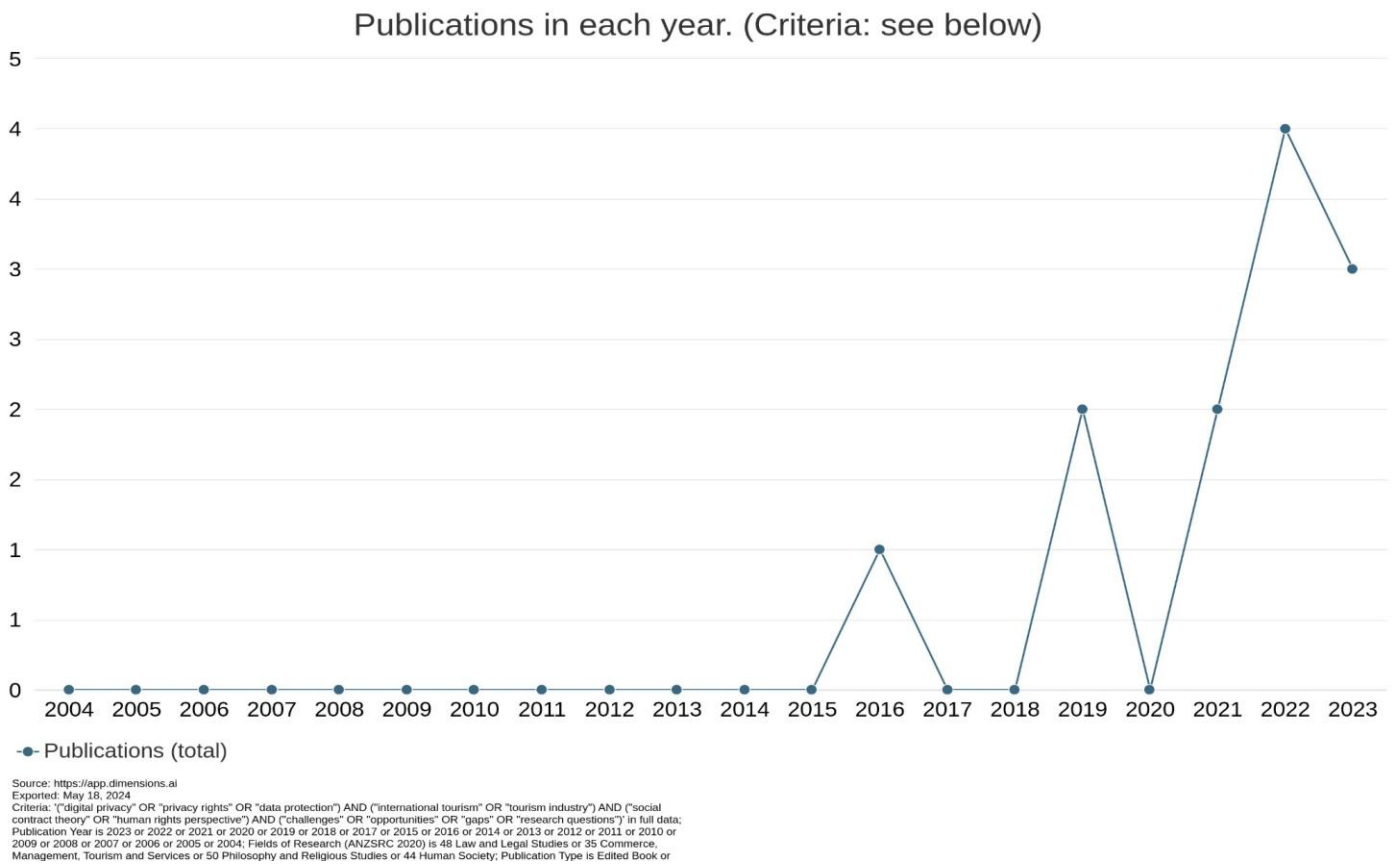


Figure 2. No. of publications published in each year.

This spike in research activity reflects a growing acknowledgment of digital privacy issues, fuelled by rapid technological advancements and heightened consumer awareness.

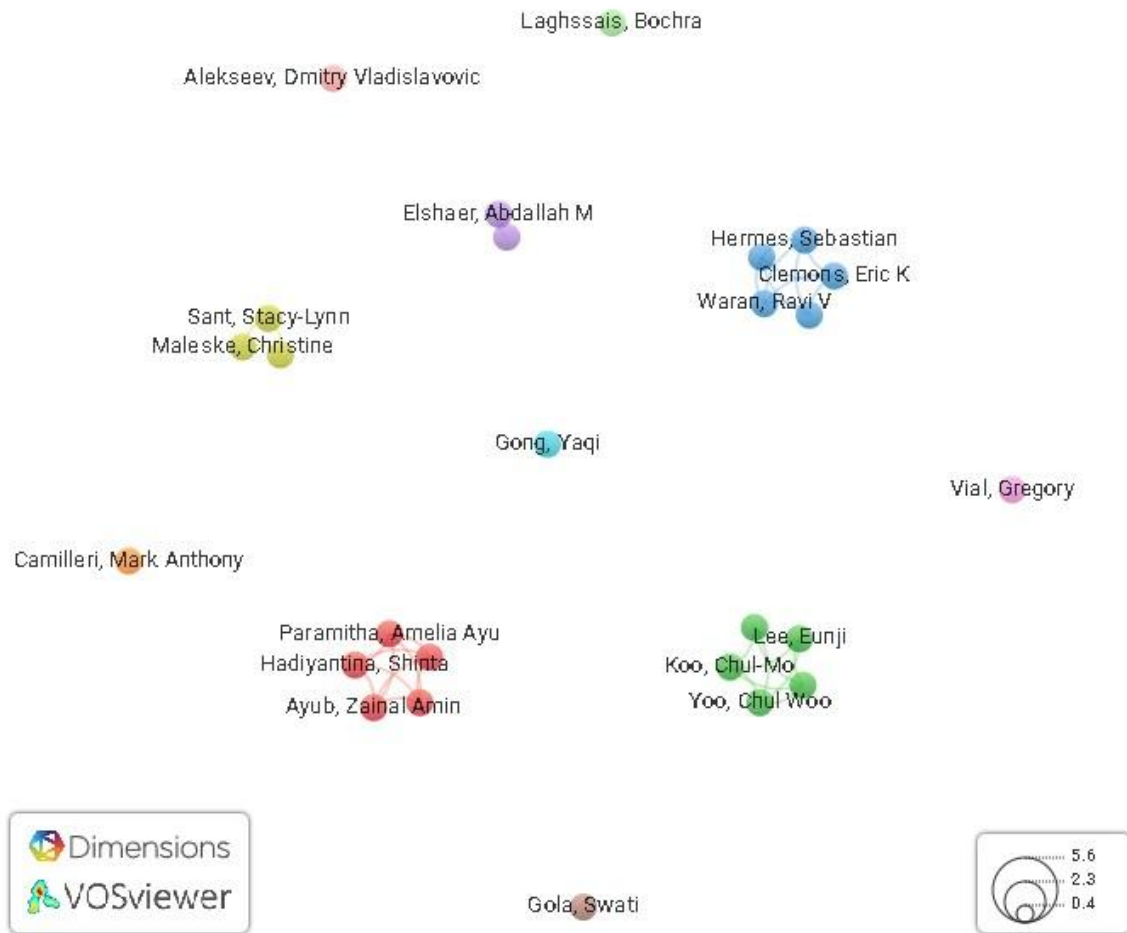


Figure 3. No. of co-authored publications.

The institutional collaboration network (**Figure 3**) highlights key universities like HEC Montréal, the University of Brawijaya, the University of South Carolina, and the University of Pennsylvania as pivotal contributors to the field. Their prominent positions suggest these institutions are hubs of research activity, likely producing influential studies that shape the academic landscape. Conversely, universities such as Kyung Hee University and the University of Michigan – Ann Arbor, while present, exhibit fewer collaborations, pointing to potential opportunities for expanding research networks.

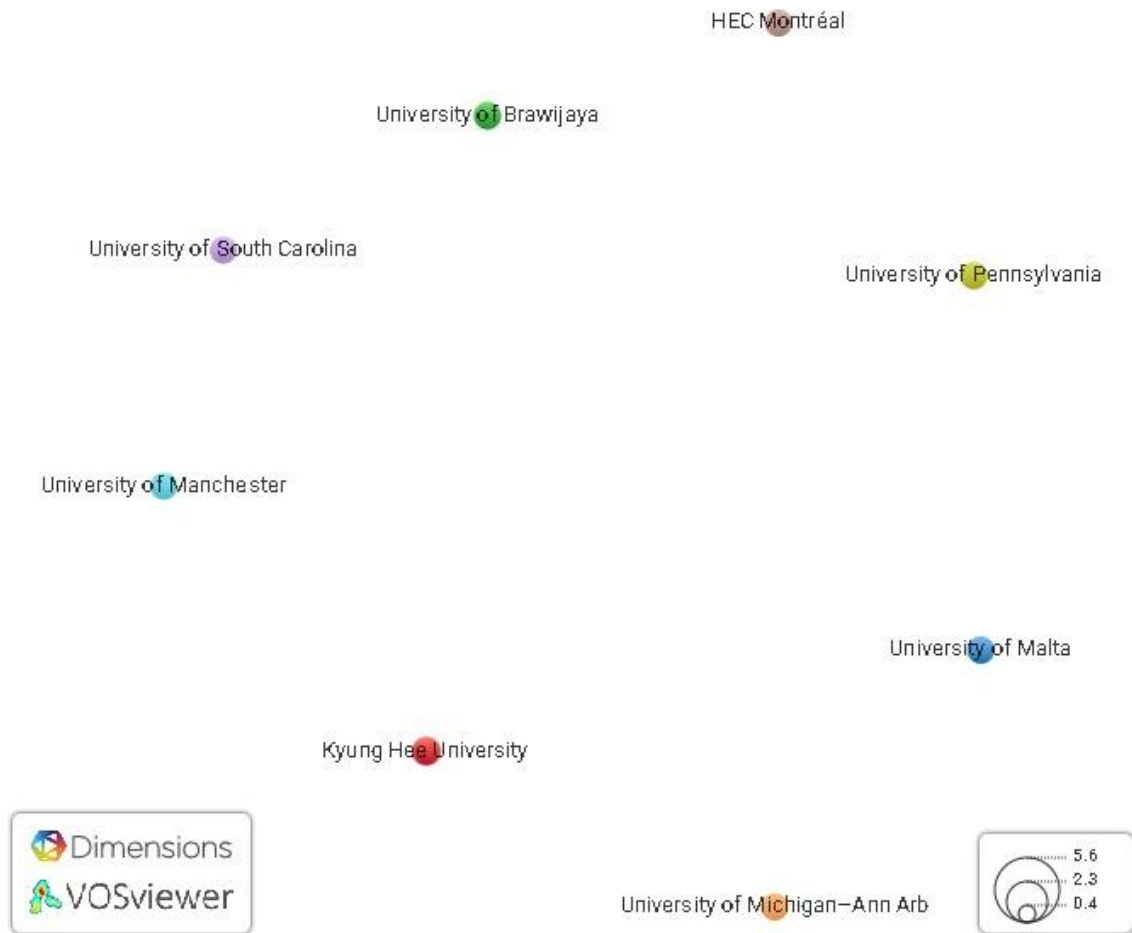


Figure 4. No of research organizations publication based on their number of co-authored publications.

The analysis of publication and citation data across journals in **Table 1** provides additional insights into the impact of research on digital privacy in tourism management. The Journal of Strategic Information Systems stands out with an exceptionally high citation count and mean, indicating a publication of significant influence. Similarly, journals such as Sustainable Development and Tourism Management Perspectives also contribute notably to the field, suggesting that research on digital privacy is being recognized and cited within broader contexts of sustainability and tourism management.

Table 1. The relatedness of source titles is determined based on the number of times they cite each other.

ID	Name	Publications	Citations	Citations (mean)
jour.1136439	Electronic Markets	1	6	6
jour.1136609	Information Systems Frontiers	1	0	-
jour.1139379	The Journal of Strategic Information Systems	1	2558	2558
jour.1140704	Sport Management Review	1	1	1
jour.1143079	Tourism Management Perspectives	1	7	7
jour.1145180	Journal of International Trade Law and Policy	1	9	9

jour.1149755	Izvestia of Saratov University Sociology Politology	1	0	-
jour.1430628	Journal of International Studies	1	0	-
jour.1431119	Sustainable Development	1	80	80

Table 2. No of published publications in each year for the selected publishers.

Name	Publications	Citations	Citations (mean)
Taylor & Francis	3	211	70.33
Elsevier	2	2565	1282.5
Springer Nature	2	6	3
Emerald	1	9	9
Saratov State University	1	0	-
UUM Press, Universiti Utara Malaysia	1	0	-
Wiley	1	80	80

Moreover, the analysis of publisher data reveals that Elsevier and Wiley are leading sources of high-impact publications in this area (see **Table 2**). Elsevier, in particular, shows a remarkable citation count and mean, underscoring the prominence and influence of its published research. Taylor & Francis also demonstrate significant impact, with a substantial number of citations across multiple publications. This trend highlights the importance of these publishers in disseminating pivotal research findings that shape the discourse on digital privacy in tourism management.

It is evident that the interplay between digital privacy and tourism management is a burgeoning area of interest. Scholars such as Buhalis and Law (2008) have underscored the transformative impact of technology on tourism, emphasizing the need for rigorous privacy protections as digital tools become ubiquitous in the industry. The growing body of research reflected in the publication trends aligns with concerns raised by Tussyadiah and Wang (2016), who highlighted the privacy risks associated with the increasing use of mobile and digital platforms in tourism.

The collaborative networks revealed in the co-author and institutional analyses resonate with calls for interdisciplinary approaches in addressing digital privacy challenges. As suggested by Puhretmair, Adamer, and Schmoelz (2018), integrating perspectives from information systems, legal studies, and tourism management can lead to more comprehensive and effective privacy solutions. The observed clusters of authors and institutions in the visualizations indicate that such interdisciplinary collaborations are indeed taking shape, fostering innovative research that addresses the multifaceted nature of digital privacy in tourism.

The provided visualizations and data underscore a dynamic and evolving research landscape in digital privacy and tourism management. The increasing publication trends, coupled with robust collaborative networks and impactful publications, reflect a growing academic engagement with critical issues at the intersection of technology and tourism. This engagement is essential in addressing the complex privacy challenges that arise in an increasingly digitalized tourism industry, ultimately contributing to more secure and sustainable tourism practices.

To further explore the research, themes analysis was utilised to demarcate the study findings into two critical scenarios, application of bridging mechanisms to reduce or alleviate issues bordering on digital privacy, or to be laissez-faires about it. In policy studies, actions or inaction, are considered in decision-making and the consequences thereof, are also well understood. Within this study, there are two major scenarios, technological utopia and data dystopia.

Scenario 1: "Technological Utopia" - A future where advanced encryption technologies and strict privacy regulations ensure robust protection of tourists' digital privacy rights.

Scenario 2: "Data Dystopia" - A future where lax regulations and pervasive data collection practices lead to widespread privacy breaches and abuses in international tourism.

Scenario 1: Technological Utopia

In this scenario, technological advancements and stringent privacy regulations create an environment where tourists' digital privacy rights are effectively protected:

- **Advanced Encryption Technologies:** Cutting-edge encryption technologies, such as quantum cryptography, blockchain, and secure multi-party computation, are widely adopted across the tourism industry. These technologies ensure that tourists' personal data remains encrypted and secure throughout its lifecycle, minimizing the risk of unauthorized access or data breaches.
- **Strict Privacy Regulations:** Governments and regulatory bodies enact and enforce robust privacy laws and regulations specifically tailored to the tourism sector. These regulations impose strict requirements on tourism organizations regarding data collection, processing, storage, and sharing. Organizations are required to obtain explicit consent from tourists before collecting their personal data and are held accountable for any breaches or violations.
- **Transparency and Accountability:** Tourism organizations prioritize transparency and accountability in their data practices. They provide clear and accessible privacy policies that outline how personal data is collected, used, and protected. Organizations undergo regular audits and assessments to ensure compliance with privacy regulations, and stringent penalties are imposed on those found to be in violation.
- **Empowered Tourists:** Tourists have a high degree of control over their personal data and are empowered to make informed decisions about its use. They have access to user-friendly privacy settings and tools that allow them to manage their privacy preferences and consent settings across different platforms and services.
- **Trust and Confidence:** The combination of advanced encryption technologies, strict privacy regulations, transparency, and user empowerment fosters a climate of trust and confidence among tourists. They feel reassured that their digital privacy rights are respected and protected, leading to increased trust in the tourism industry and higher levels of engagement with digital platforms and services.

Scenario 2: Data Dystopia

In contrast, Scenario 2 paints a bleak picture where lax regulations and pervasive data collection practices undermine tourists' digital privacy rights:

- **Weak Regulatory Framework:** Governments and regulatory bodies fail to enact or enforce adequate privacy laws and regulations for the tourism sector. There is

a lack of clear guidelines and oversight regarding data collection, processing, and sharing practices, leaving tourists vulnerable to exploitation and abuse.

- **Pervasive Data Collection:** Tourism organizations engage in pervasive and indiscriminate data collection practices, harvesting vast amounts of personal data from tourists without their knowledge or consent. This includes sensitive information such as biometrics, geolocation data, and behavioral patterns, which are used for targeted advertising, profiling, and surveillance purposes.
- **Data Breaches and Exploitation:** The absence of robust security measures and accountability mechanisms results in frequent data breaches and abuses. Tourists' personal data is routinely compromised, leading to identity theft, financial fraud, and other forms of exploitation. Organized cybercriminal groups exploit vulnerabilities in tourism systems to steal and monetize tourists' personal information on the dark web.
- **Erosion of Trust:** Widespread privacy breaches and abuses erode tourists' trust and confidence in the tourism industry. They become reluctant to share their personal information or engage with digital platforms and services out of fear of privacy violations. Negative publicity and media coverage further exacerbate the erosion of trust, tarnishing the reputation of tourism organizations and destinations.
- **Legal and Ethical Concerns:** Civil society groups and privacy advocates raise alarm bells about the erosion of digital privacy rights in international tourism. They call for urgent regulatory reforms and ethical standards to address the growing threat of data dystopia and safeguard tourists' rights in the digital age.
- While Scenario 1 presents a vision of a technologically advanced and privacy-respecting future for international tourism, Scenario 2 depicts a dystopian reality characterized by privacy breaches, exploitation, and erosion of trust. These scenarios serve as thought-provoking narratives that highlight the importance of proactive measures to protect tourists' digital privacy rights and ensure a positive and secure tourism experience for all.

Proactive solutions to tourist data privacy right amid technological advancement

The tourism industry faces increasing challenges in managing personal data privacy. As tourists engage with digital platforms, the need for robust technological solutions and regulatory frameworks is critical. Tourism businesses must adopt cutting-edge technologies to protect user data while complying with regulatory standards. This essay explores potential solutions, highlighting the role of emerging technologies and regulatory frameworks, offering practical examples for improving digital privacy in tourism.

One promising solution is blockchain technology, which enhances data security and transparency. Blockchain's decentralized nature ensures data integrity by creating an immutable ledger (Zheng et al., 2018). In tourism, this technology can give tourists control over personal data through decentralized identity management. Platforms like LockTrip have demonstrated blockchain's potential, using smart contracts to ensure personal data is only shared when necessary, reducing breaches (Li et al., 2018).

Another crucial technology is end-to-end encryption, which secures sensitive data like payment information. Major platforms like Expedia Group use encryption to protect customer data during transactions, minimizing vulnerabilities (Gursoy et al.,

2019). By securing data exchanges, tourism companies can build trust with consumers who are increasingly concerned about how their data is handled (Li et al., 2023; Rahmouni et al., 2019). Privacy-preserving AI also offers solutions, especially with federated learning, which allows AI models to learn from data without centralizing it, preserving user privacy (McMahan et al., 2017). For example, Google's Travel Service uses federated learning to offer personalized recommendations without exposing user data. This innovation demonstrates how AI can enhance services while respecting privacy (Bonawitz et al., 2019). Adopting a zero-trust security architecture is another effective approach. This model continuously verifies users and devices, assuming no one can be trusted by default (Kindervag, 2010). Airbnb, for instance, uses multi-factor authentication and continuous monitoring to safeguard customer data, reducing unauthorized access (Park & Kim, 2018). Data anonymization further protects privacy by removing personally identifiable information from datasets. Booking.com uses this technique to analyze customer behavior without compromising privacy, enabling personalized services while ensuring data security (Sweeney, 2002).

From a regulatory standpoint, the General Data Protection Regulation (GDPR) in the European Union has set high standards for data protection, requiring explicit consent from users and limiting data transfers outside the EU (Voigt & Von dem Bussche, 2017). Tourism companies like Marriott have improved their data protection systems to comply with GDPR, ensuring secure cross-border data transfers (Calders & Pechenizkiy, 2020). Mandatory privacy audits under GDPR ensure businesses continuously improve their security practices (Fang, 2023). Companies like Marriott undergo regular audits, which foster consumer trust by demonstrating commitment to protecting personal data (Goddard, 2017). The Privacy by Design and Privacy by Default principles also strengthen data protection. These principles require businesses to prioritize privacy at every stage of product development. For example, Apple's Safari browser blocks third-party cookies, ensuring privacy without user intervention (Cavoukian, 2010). Harmonizing global data protection regulations, such as the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System, would simplify compliance for tourism companies, ensuring consistent protection across jurisdictions (Greenleaf, 2014).

Overall, tourism businesses must combine emerging technologies and regulatory frameworks to address digital privacy concerns. Blockchain, encryption, and privacy-preserving AI offer robust technological solutions, while GDPR and Privacy by Design principles provide essential legal protections. By learning from real-world examples like Marriott's GDPR efforts and Google's federated learning model, the tourism industry can build a secure, privacy-respecting environment for travelers.

5. Summary of findings

The provided visualizations and data reveal significant trends and patterns in the publication landscape concerning digital privacy within tourism management. These insights, when juxtaposed with existing literature, paint a comprehensive picture of the evolving academic discourse in this field.

From 2004 to 2023, there has been a notable surge in publications on digital privacy and tourism management, particularly from 2015 onward. The year 2022 saw

the highest number of publications, with five, followed by four in 2021 and three in 2023. This trend reflects a growing acknowledgment of digital privacy issues, driven by technological advancements and increased consumer awareness. Buhalis and Amaranggana (2015) emphasize that digital transformation in tourism requires robust privacy measures to protect user data, while Bec, Moyle, Schaffer & Timms (2021) highlight the need for stringent data protection practices due to the rising reliance on mobile technologies. These studies underscore the industry's recognition of digital privacy as a crucial concern.

Network visualizations of co-authors (**Figure 2**) and institutions (**Figure 3**) highlight the collaborative nature of research in digital privacy within tourism management. Prominent clusters of authors, such as Hermes, Sebastian, Clemons, Eric K., and Waran, Ravi V., suggest active networks driving innovation through diverse, interdisciplinary contributions, fostering robust academic discourse. However, some authors and institutions appear more isolated, indicating areas where increased collaboration could enhance research impact.

The institutional collaboration network identifies key universities like HEC Montréal, University of Brawijaya, University of South Carolina, and University of Pennsylvania as pivotal contributors, producing influential studies that shape the academic landscape. Conversely, universities such as Kyung Hee University and the University of Michigan–Ann Arbor exhibit fewer collaborations, suggesting opportunities for expanding research networks. Furthermore, Katz and Martin (1997) underscore the value of collaborative research in enhancing scientific output. These clusters reflect interdisciplinary efforts crucial for addressing complex issues like digital privacy in tourism, aligning with Puhretmair, Adamer, and Schmoelz (2018), who advocate for integrating diverse perspectives to develop comprehensive privacy solutions in tourism.

The analysis of publication and citation data across journals (see **Table 1**) provides additional insights into the impact of research on digital privacy in tourism management. The *Journal of Strategic Information Systems* stands out with an exceptionally high citation count and mean, indicating a publication of significant influence. Similarly, journals such as *Sustainable Development* and *Tourism Management Perspectives* also contribute notably to the field, suggesting that research on digital privacy is being recognized and cited within broader contexts of sustainability and tourism management. Recent studies, such as those by Cavusoglu, Mishra, and Raghunathan (2015), have shown that publications in high-impact journals significantly influence subsequent research and policy-making. The high citation counts observed in the *Journal of Strategic Information Systems* and other influential journals corroborate the importance and impact of research on digital privacy within the broader academic and policy-making communities.

The analysis of publisher data reveals that Elsevier and Wiley (see **Table 2**) are leading sources of high-impact publications in digital privacy within tourism management. Elsevier, in particular, shows a remarkable citation count and mean, underscoring its prominence and influence. Taylor & Francis also demonstrate significant impact, with substantial citations across multiple publications. This trend highlights the importance of these publishers in shaping the discourse on digital privacy in tourism management.

The role of publishers in disseminating impactful research is well-documented. According to Tenopir and King (2000), the reputation and reach of prominent publishers like Elsevier and Wiley significantly enhance the visibility and impact of research. The high citation counts associated with these publishers reflect their crucial role in advancing the discourse on digital privacy in tourism management.

Findings from the visualizations and data underscore a dynamic and evolving research landscape. Increasing publication trends, coupled with robust collaborative networks and impactful publications, reflect growing academic engagement with critical issues at the intersection of technology and tourism, addressing complex privacy challenges and contributing to more secure and sustainable tourism practices.

6. Discussion

In examining the publication patterns, collaborative networks, and citation statistics in the field of digital privacy in tourism management, the result uncovers a dynamic and fast changing research environment. Results shows that there has been a significant rise in publications since 2015, reaching its highest point in 2022, indicating an increasing understanding and acknowledgment of the crucial significance of digital privacy in the tourism sector. This increase is strongly relevant to the wider discussion on the revolutionary influence of digital technology on the tourism industry (Buhalis and Amaranggana, 2015; Ndaguba, 2024; Bec, Moyle, Schaffer & Timms 2021). These academics stress the need of establishing strong privacy protocols to safeguard user data, which aligns with the concepts of social contract theory that prioritize mutual trust and the preservation of individual rights.

The surge in scholarly production not only signifies a rise in academic interest but also demonstrates the industry's acknowledgment of the intricate privacy issues brought about by digitalization. The study conducted by Cavusoglu, Mishra, and Raghunathan (2015) highlights the substantial influence of privacy violations on the reputation and market worth of companies. This fact further emphasizes the need of implementing strong privacy safeguards in the contemporary digital economy. The worries expressed are also reflected in the tourism industry, where the necessity for strict data privacy measures is intensified by the widespread use of mobile and digital platforms (Gretzel, Sigala, Xiang, & Koo, 2015). The network-based representations of collaborative endeavors across authors and institutions indicate that the integration of several disciplines is stimulating creativity in tackling these issues. The predominance of clusters featuring scholars such as Hermes, Sebastian, Clemons, and Waran highlight the advantages of combining knowledge from many fields, such as information systems, legal studies, and tourism management. These collaborations might be regarded as joint endeavors to preserve the implicit agreements between visitors and organizations, which are fundamental to preserving trust in the era of digital technology. Katz and Martin (1997) argue that such collaborations serve to augment scientific productivity and foster innovation. This phenomenon is prominently observed in the multidisciplinary character of digital privacy research in the tourism industry.

The theory of social contract offers a strong intellectual foundation for comprehending these tacit agreements. The hypothesis suggests that tourists anticipate

their personal data to be managed with transparency, permission, and accountability in return for the services rendered by enterprises. This is especially pertinent in situations such as "Technological Utopia," where sophisticated technology and strict requirements protect privacy, and "Data Dystopia," when the lack of such controls results in privacy violations and a subsequent decline in confidence (Floridi, 2014). The divergent situations highlight the urgent necessity for implementation of proactive strategies to safeguard the digital privacy rights of tourists.

Furthermore, the substantial number of citations and the influence of prominent publications such as the *Journal of Strategic Information Systems and Sustainable Development* highlight the importance of this research in scientific discussions and the formulation of practical policies. Highly influential articles, such as those authored by De Hert and Gutwirth (2006), have a vital function in influencing the policy environment by emphasizing the legal and ethical consequences of privacy in digital environments. The prominent status and impact of these publications underscore the need of ongoing study and scholarly involvement in this domain.

In the dissemination of influential research, the contribution of publishers such as Elsevier and Wiley cannot be exaggerated. Tenopir and King (2000) observe that the reputation and extensive reach of these publishers greatly increase the prominence and influence of research. Particularly crucial in the domain of digital privacy in tourism is the distribution of research findings through reputable publications to ensure that the most recent research reaches policymakers, industry leaders, and other stakeholders who have the responsibility of implementing efficient privacy safeguards.

The evolving research environment in digital privacy within tourism management reflects an increasing recognition from both academia and industry of the challenges presented by digital technologies. Through the lens of social contract theory, scholars like Voigt & Von dem Bussche (2017) emphasize the importance of transparency, consent, and accountability in data practices. These principles are foundational to maintaining trust and collaboration between tourists and tourism organizations. Blockchain, AI, and encryption technologies fulfill the expectations that tourists have under the social contract by ensuring that their personal data is protected and used responsibly (Zheng et al., 2018; Bonawitz et al., 2019). Any breach of this trust—whether due to weak privacy measures or failure to comply with regulations—undermines this social contract, leading to reputational damage, loss of consumer loyalty, and long-term sustainability risks for tourism organizations (Cavusoglu, Mishra, & Raghunathan, 2015). In contrast, organizations that proactively adopt strong privacy frameworks are more likely to foster sustained trust and collaboration, reinforcing the social contract (Gong & Schroeder, 2022).

The "Technological Utopia" and "Data Dystopia" scenarios illustrate the potential future outcomes based on the industry's approach to managing digital privacy. Technological Utopia represents a future where organizations implement advanced privacy technologies, enforce robust privacy regulations, and ensure transparency and accountability in their data practices. This scenario highlights how trust is strengthened, benefiting both consumers and organizations (Pencarelli, 2020). On the other hand, Data Dystopia depicts the negative consequences of failing to prioritize privacy, where weak regulations lead to data breaches, trust erosion, and damage to organizational reputations (Johnson & Verdicchio, 2023; Zuboff, 2023). These

contrasting scenarios clearly demonstrate how the social contract between tourists and organizations can either be upheld or violated, depending on the steps taken by industry leaders and policymakers.

To achieve Technological Utopia, industry leaders must adopt cutting-edge technologies such as blockchain and privacy-preserving AI (Bonawitz et al., 2019; Li et al., 2023), alongside robust regulatory frameworks that protect tourists' data. Policymakers, in turn, have a crucial role in enforcing global privacy standards (Greenleaf, 2021), ensuring that tourism organizations adhere to the expectations of transparency and consent. Failing to take these proactive steps risks leading the industry into Data Dystopia, where privacy violations weaken the trust that forms the basis of the digital economy. The flow between these scenarios and practical recommendations makes it clear that safeguarding tourists' information not only upholds the social contract but also increases consumer loyalty and positions organizations for long-term success in the digital marketplace.

In sum, social contract theory serves as both a theoretical framework and a practical guide for understanding how tourism organizations must balance their responsibilities to tourists. By implementing privacy-enhancing technologies and adhering to global privacy regulations, organizations can maintain the integrity of this contract, securing consumer trust and loyalty (Voigt & Von dem Bussche, 2017). Policymakers are urged to create robust, forward-thinking regulations that reinforce these privacy measures, while industry leaders are called to adopt advanced data protection technologies that ensure transparency and accountability. Real-world examples, such as Marriott's compliance with GDPR, demonstrate how these actions can prevent breaches and bolster organizational trust (Ebuzor, 2023; Di Lena, 2023). Furthermore, future research should explore tourists' perspectives on privacy, as well as how global regulatory frameworks can be harmonized to better protect personal data across borders. By addressing these gaps, the study opens the door to a more secure and privacy-conscious tourism industry.

7. Conclusions

Theoretical contribution

This research contributes to the existing theory of social contract by extending its application to the contemporary context of digital privacy within tourism management. Traditionally, social contract theory, as developed by philosophers such as Thomas Hobbes, John Locke, and Jean-Jacques Rousseau, focuses on the implicit agreements between individuals and governing institutions, where individuals consent to certain regulations and protections in exchange for societal benefits and security. This study expands the theory's scope to include the digital realm, specifically addressing the relationships and expectations between tourists and tourism organizations regarding the handling of personal data.

The analysis of publication trends, collaborative networks, and citation data underscores the evolving nature of these implicit agreements in the digital age. By highlighting the significant increase in scholarly output related to digital privacy in tourism, this research demonstrates a growing recognition of the need for new norms and protections that align with technological advancements. This aligns with the social

contract's premise that as societal conditions change, so must the agreements and protections that govern them. The interdisciplinary collaborations revealed through network visualizations further reinforce the idea that addressing complex, modern issues like digital privacy requires collective efforts and shared expertise, reflecting the social contract's emphasis on mutual benefit and cooperation.

Furthermore, the study's exploration of scenarios such as "Technological Utopia" and "Data Dystopia" provides a nuanced understanding of how different regulatory environments can either uphold or undermine the social contract in the digital age. In a "Technological Utopia," advanced encryption technologies and strict privacy regulations create a secure environment for tourists, ensuring that organizations fulfill their obligations under the social contract. Conversely, a "Data Dystopia" scenario highlights the consequences of failing to adapt to new digital realities, where lax regulations lead to widespread privacy breaches and a breakdown of trust. By emphasizing the need for transparency, consent, fairness, and accountability in data practices, this research reinforces the social contract's core principles and underscores the necessity of evolving these principles to address the challenges posed by digital transformation in tourism. Thus, this study not only applies social contract theory to a new context but also enriches it by demonstrating how its principles can guide the development of fair and effective data privacy practices in the digital age.

Practical implication

Understanding the rapidly evolving landscape of digital privacy within tourism management is not merely an academic exercise; it holds profound implications for how we approach the protection of personal data in a globalized, technology-driven world. As digital technologies continue to revolutionize the tourism industry, the need for robust privacy measures becomes ever more critical. The surge in scholarly research reflects an industry-wide recognition that safeguarding digital privacy is not just a regulatory obligation but a fundamental component of maintaining consumer trust and ensuring the long-term sustainability of tourism practices.

The application of social contract theory to digital privacy in tourism underscores the ethical and practical necessity of transparency, consent, and accountability in data practices. By framing the relationship between tourists and organizations as an implicit social contract, we can better understand the mutual responsibilities that exist in the digital age. This understanding drives home the importance of interdisciplinary research and collaboration, as highlighted by the network visualizations, which show that solving these complex challenges requires pooling expertise from diverse fields.

Moreover, the prominence of high-impact publications and the influence of major publishers in disseminating research highlight the importance of visibility and accessibility in advancing the discourse on digital privacy. This research does not exist in a vacuum; it directly influences policy-making, industry standards, and ultimately, the protection of individual rights in the digital sphere.

In practical terms, this means that the tourism industry, policymakers, and academic researchers must continue to work together to develop and implement privacy solutions that are not only effective but also adaptable to the rapid pace of technological change. The ongoing academic engagement in this field is crucial for keeping pace with emerging threats and opportunities, ensuring that the rights of tourists are respected and protected in an increasingly digital world.

Thus, the significance of this discussion lies in its potential to shape the future of digital privacy in tourism. By understanding and acting upon these insights, stakeholders can foster a more secure, trustworthy, and sustainable tourism industry that benefits both individuals and society as a whole.

For Policymakers:

The study highlights the urgent need for robust regulatory frameworks that enforce stringent data privacy protections. Policymakers can use these findings to craft and implement comprehensive privacy laws that mandate transparency, consent, and accountability in data handling practices. This could include regulations requiring explicit consent from tourists before collecting their data, regular audits of data practices, and stringent penalties for violations. By doing so, policymakers can create a secure digital environment that upholds the social contract, ensuring that tourists' digital privacy rights are respected and protected.

For Tourism Organizations:

Tourism organizations are at the forefront of handling vast amounts of personal data, and this research underscores their responsibility in upholding the principles of the social contract. Organizations should adopt advanced encryption technologies and establish clear, accessible privacy policies that explain how data is collected, used, and protected. They should also implement user-friendly privacy settings that empower tourists to manage their data preferences. By prioritizing transparency, consent, and accountability, tourism organizations can foster trust and confidence among tourists, enhancing their reputation and customer loyalty. Additionally, organizations can benefit from regular training and updates on best practices in data privacy to ensure ongoing compliance with evolving regulations.

For Technology Developers:

Developers of digital platforms and applications used in the tourism industry play a crucial role in implementing effective privacy measures. The study suggests the integration of cutting-edge encryption technologies such as blockchain and secure multi-party computation to ensure data security. Developers should focus on creating tools and interfaces that make it easy for users to control their privacy settings and understand how their data is being used. By embedding privacy by design into their products, technology developers can help tourism organizations comply with regulations and meet tourists' expectations for data privacy.

Future directions

Future research should focus on interdisciplinary collaborations, longitudinal studies, and consumer behavior analysis to enhance digital privacy in tourism management. Developing advanced encryption technologies, ethical frameworks, and robust policy assessments will be crucial. Investigating the impact of emerging technologies like AI and IoT, alongside educational initiatives, can raise awareness and improve data protection practices. Global collaborations and improved user experience design will also be vital. These efforts will help create a secure digital environment, ensuring that the principles of social contract theory are upheld, fostering trust and cooperation in the tourism industry.

Conflict of interest: The authors declare no conflicts of interest.

References

- Buhalis, D., & Amaranggana, A. (2015). Smart tourism destinations enhancing tourism experience through personalisation of services. *Information and Communication Technologies in Tourism 2015*, 377–389. https://doi.org/10.1007/978-3-319-14343-2_29 https://doi.org/10.1007/978-3-319-14343-9_28
- Buhalis, D., & Law, R. (2008). Progress in information technology and tourism management: 20 years on and 10 years after the Internet—The state of eTourism research. *Tourism Management*, 29(4), 609–623. <https://doi.org/10.1016/j.tourman.2008.01.005>
- Cavoukian, A. (2010). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, Canada.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2015). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1), 69–104. <https://doi.org/10.2753/JEC1086-4415090101> <https://doi.org/10.1080/10864415.2004.11044320>
- De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In *Privacy and the criminal law* (pp. 61–104). Intersentia.
- Andersen, I. M. V., Blichfeldt, B. S., & Liburd, J. J. (2016). Sustainability in coastal tourism development: an example from Denmark. *Current Issues in Tourism*, 21(12), 1329–1336. <https://doi.org/10.1080/13683500.2016.1272557>
- Floridi, L. (2014). Open Data, Data Protection, and Group Privacy. *Philosophy & Technology*, 27(1), 1–3. <https://doi.org/10.1007/s13347-014-0157-8>
- Gretzel, U., Sigala, M., Xiang, Z., et al. (2015). Smart tourism: foundations and developments. *Electronic Markets*, 25(3), 179–188. <https://doi.org/10.1007/s12525-015-0196-8>
- Johnson, D. G., & Verdicchio, M. (2018). AI, agency and responsibility: the VW fraud case and beyond. *AI & SOCIETY*, 34(3), 639–647. <https://doi.org/10.1007/s00146-017-0781-9>
- Katz, J. S., & Martin, B. R. (1997). What is research collaboration? *Research Policy*, 26(1), 1–18. [https://doi.org/10.1016/S0048-7333\(96\)00917-1](https://doi.org/10.1016/S0048-7333(96)00917-1)
- Izurieta, G., Torres, A., Patiño, J., et al. (2021). Exploring community and key stakeholders' perception of scientific tourism as a strategy to achieve SDGs in the Ecuadorian Amazon. *Tourism Management Perspectives*, 39, 100830. <https://doi.org/10.1016/j.tmp.2021.100830>
- Banks, J., & de Graaf, M. (2020). Toward an Agent-Agnostic Transmission Model: Synthesizing Anthropocentric and Technocentric Paradigms in Communication. *Human-Machine Communication*, 1, 19–36. Portico. <https://doi.org/10.30658/hmc.1.2>
- Tyan, I., Guevara-Plaza, A., & Yagüe, M. I. (2021). The Benefits of Blockchain Technology for Medical Tourism. *Sustainability*, 13(22), 12448. <https://doi.org/10.3390/su132212448>
- Puhretmair, F., Adamer, D., & Schmoelz, C. (2018). Bridging the digital divide: A barrier-based approach. In *Social Inclusion: Societal and Organizational Implications for Information Systems* (pp. 87–104). Springer Cham. https://doi.org/10.1007/978-3-319-14343-2_15
- Rawls, J. (1971). *A Theory of Justice*. <https://doi.org/10.4159/9780674042605>
- Pencarelli, T. (2019). The digital revolution in the travel and tourism industry. *Information Technology & Tourism*, 22(3), 455–476. <https://doi.org/10.1007/s40558-019-00160-3>
- Tenopir, C., King, D. W., & Campbell, R. (2000). Towards electronic journals: realities for scientists, librarians & publishers. *Journal of Scholarly Publishing*, 31(4), 214.
- Gong, Y., & Schroeder, A. (2022). A systematic literature review of data privacy and security research on smart tourism. *Tourism Management Perspectives*, 44, 101019. <https://doi.org/10.1016/j.tmp.2022.101019>
- Bec, A., Moyle, B., Schaffer, V., et al. (2021). Virtual reality and mixed reality for second chance tourism. *Tourism Management*, 83, 104256. <https://doi.org/10.1016/j.tourman.2020.104256>
- Tussyadiah, I. P., & Wang, D. (2014). Tourists' Attitudes toward Proactive Smartphone Systems. *Journal of Travel Research*, 55(4), 493–508. <https://doi.org/10.1177/0047287514563168>
- Xiang, Z., Magnini, V. P., & Fesenmaier, D. R. (2015). Information technology and consumer behavior in travel and tourism: Insights from travel planning using the internet. *Journal of Retailing and Consumer Services*, 22, 244–249. <https://doi.org/10.1016/j.jretconser.2014.08.005>

- Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>
- Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., & McMahan, B. (2019). Towards federated learning at scale: System design. *Proceedings of Machine Learning and Systems*, 2, 374–388.
- Calders, T., & Pechenizkiy, M. (2020). Fairness-aware data mining: A survey. *International Journal of Data Science and Analytics*, 9(2), 75–94.
- Cavoukian, A. (2010). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario*, 5(1), 12–23.
- Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, 59(6), 703–705. <https://doi.org/10.2501/ijmr-2017-050>
- Greenleaf, G. (2014). Global data privacy laws 2014: Four decades of growth, but uneven globalization. *Journal of Law and Information Science*, 31(1), 181–233.
- Gursoy, D., Chi, C.G., & Lu, L. (2019). Privacy concerns and the use of biometric technology in travel. *Journal of Hospitality & Tourism Research*, 43(3), 417–437.
- Kindervag, J. (2010). No more chewy centers: Introducing the zero trust model of information security. Forrester Research.
- Li, S., Karahanna, E., & Xu, S. (2018). The influence of privacy concerns on citizens' adoption of e-government services: An extension of the privacy calculus model. *Journal of Strategic Information Systems*, 27(1), 92–111.
- McMahan, H.B., Moore, E., Ramage, D., & Hampson, S. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of Artificial Intelligence and Statistics*, 54, 1273–1282.
- Park, S., & Kim, J. (2018). The impact of security awareness on trust in social networking services: A study on Airbnb users. *International Journal of Information Management*, 43, 210–223.
- Rahmouni, K., Lefebvre, B., & Lu, C. (2019). End-to-end encrypted communication for secure data exchange in smart tourism. *Tourism Management*, 70, 134–144.
- SWEENEY, L. (2002). ACHIEVING k-ANONYMITY PRIVACY PROTECTION USING GENERALIZATION AND SUPPRESSION. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05), 571–588. <https://doi.org/10.1142/s021848850200165x>
- Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-57959-7>
- Zheng, Z., Xie, S., Dai, H. N., et al. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 14(4), 352. <https://doi.org/10.1504/ijwgs.2018.095647>
- Ifeoluwa Oreofe Adekuajo, Ololade Gilbert Fakeyede, Chioma Ann Udeh, & Chibuike Daraojimba. (2023). THE DIGITAL EVOLUTION IN HOSPITALITY: A GLOBAL REVIEW AND ITS POTENTIAL TRANSFORMATIVE IMPACT ON U.S. TOURISM. *International Journal of Applied Research in Social Sciences*, 5(10), 440–462. <https://doi.org/10.51594/ijarss.v5i10.633>
- Collado-Agudo, J., Herrero-Crespo, Á., & San Martín-Gutiérrez, H. (2023). The adoption of a smart destination model by tourism companies: An ecosystem approach. *Journal of Destination Marketing & Management*, 28, 100783. <https://doi.org/10.1016/j.jdmm.2023.100783>
- Shah, I. A., Jhanjhi, N. Z., & Brohi, S. (2024). Cybersecurity Issues and Challenges in Civil Aviation Security. *Cybersecurity in the Transportation Industry*, 1–23. Portico. <https://doi.org/10.1002/9781394204472.ch1>
- Babin, B. J., & Harris, E. G. (2023). *CB Consumer behaviour*. Cengage Canada.
- Gustafsson, D. (2023). *The Present People*.
- Idowu, S. O., Schmidpeter, R., Capaldi, N., et al. (Eds.). (2023). *Encyclopedia of Sustainable Management*. <https://doi.org/10.1007/978-3-031-25984-5>
- Lee, N. J. (2024). Freedom of Movement: Protecting the Right to Travel from Location Tracking Interference. *Drexel L. Rev.*, 16, 187.
- Sandbrook, C., Clark, D., Toivonen, T., et al. (2021). Principles for the socially responsible use of conservation monitoring technology and data. *Conservation Science and Practice*, 3(5). Portico. <https://doi.org/10.1111/csp.2374>
- Ortega-Rodríguez, C., Licerán-Gutiérrez, A., & Moreno-Albarracín, A. L. (2020). Transparency as a Key Element in Accountability in Non-Profit Organizations: A Systematic Literature Review. *Sustainability*, 12(14), 5834. <https://doi.org/10.3390/su12145834>

- Yıldırım, M. (2021). Tracing the consent, adaptation and resistance practices of an ‘unsustainable’ workforce: The governmentality of workplaces in tourism industry. *Tourism Management*, 84, 104260. <https://doi.org/10.1016/j.tourman.2020.104260>
- Tassikas, A. D. (2021). Data Processing and Legal Protection in Contracts in the Technologically Innovative Tourism Sector. *European Journal of Tourism, Hospitality and Recreation*, 11(1), 77–90. <https://doi.org/10.2478/ejthr-2021-0008>
- Härkönen, E. (2020). Right to privacy and tourism. *Human Rights Issues in Tourism*.
- Pangrazio, L., & Sefton-Green, J. (2021). Digital Rights, Digital Citizenship and Digital Literacy: What’s the Difference? *Journal of New Approaches in Educational Research*, 10(1), 15–27. <https://doi.org/10.7821/naer.2021.1.616>
- DeNardis, L. (2020). The Internet in Everything. <https://doi.org/10.12987/9780300249330>
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>
- Ndaguba, E., & Marais, L. (2023). A scientometric analysis of mine closure research. *Environment, Development and Sustainability*, 26(11), 27787–27803. <https://doi.org/10.1007/s10668-023-03785-x>
- Ndaguba, E., Cilliers, J., Mbanga, S., et al. (2022). Re-Imaging the Future in Urban Studies and Built Environment Discourse: A Neurourbanism Perspective. *Buildings*, 12(12), 2056. <https://doi.org/10.3390/buildings12122056>
- Ndaguba, E., Brown, K., Marinova, D., et al. (2023). Exploring the Social Impact of the Short-Stay Market (SSM) in Regional Areas: An Empirical Study. *Fudan Journal of the Humanities and Social Sciences*, 17(2), 243–277. <https://doi.org/10.1007/s40647-023-00379-9>
- Ndaguba, E., & Arukwe, C. (2024). Ecosystem of smart spaces: An overview review. *Smart Spaces*, 139–166. <https://doi.org/10.1016/b978-0-443-13462-3.00010-8>
- Bieker, F. (2022). The Right to Data Protection. In *Information Technology and Law Series*. T.M.C. Asser Press. <https://doi.org/10.1007/978-94-6265-503-4>
- Schwartz, P. M. (1994). European data protection law and restrictions on international data flows. *Iowa L. Rev.*, 80, 471.
- Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human Genetics*, 137(8), 575–582. <https://doi.org/10.1007/s00439-018-1919-7>
- Yallop, A. C., Gică, O. A., Moisescu, O. I., et al. (2021). The digital traveller: implications for data ethics and data governance in tourism and hospitality. *Journal of Consumer Marketing*, 40(2), 155–170. <https://doi.org/10.1108/jcm-12-2020-4278>
- Li, J., Wu, L., Qi, J., et al. (2023). Determinants Affecting Consumer Trust in Communication With AI Chatbots. *Journal of Organizational and End User Computing*, 35(1), 1–24. <https://doi.org/10.4018/joeuc.328089>
- Fang, S., Liu, Q., Zhang, F., et al. (2023). Application of Internet of Things and Blockchain in Information Security and Privacy Protection of Global Organizations. *Journal of Organizational and End User Computing*, 35(3), 1–16. <https://doi.org/10.4018/joeuc.323192>
- Greenleaf, G. (2021). Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3836348>
- Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-57959-7>
- Zheng, Z., Xie, S., Dai, H. N., et al. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 14(4), 352. <https://doi.org/10.1504/ijwgs.2018.095647>
- Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., & McMahan, B. (2019). Towards federated learning at scale: System design. *Proceedings of Machine Learning and Systems*, 2, 374–388.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2015). The impact of data privacy laws on trust in the digital age. *Journal of Law, Technology & Policy*, 9(1), 45–66.
- Gong, X., & Schroeder, R. (2022). Safeguarding human rights in digital tourism: Challenges and solutions. *International Journal of Tourism Management*, 54(1), 1–18.
- Pencarelli, T. (2020). Artificial intelligence and customized travel experiences: Addressing privacy issues. *Journal of Travel Research*, 59(5), 992–1007.
- Johnson, D. G., & Verdicchio, M. (2023). AI, ethics, and privacy in tourism. *Journal of Travel Research*, 62(3), 355–369.
- Zuboff, S. (2023). Surveillance capitalism and its implications for digital privacy in tourism. *Journal of Information Technology*, 38(2), 112–130.

- Retracted: Information and Data Analysis Based on Big Data and Blockchain Technology in Promoting the Development of Cultural Tourism Industry. (2023). *Security and Communication Networks*, 2023, 1–1.
<https://doi.org/10.1155/2023/9843904>
- Ebuzor, J. (2024). Good Governance and Cybersecurity. *Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector*, 112–136. <https://doi.org/10.4018/979-8-3693-2715-9.ch006>
- Di Lena, L. (2023). Data Privacy Regulation's Impact on the Global Digital Innovation Economy: An Analysis of International Regulatory Effects on the Technology Industry. *Syracuse J. Int'l L. & Com.*, 51, 119.
- Tran, H. (2024). Understanding user information behaviour: An analysis of data protection measures on digital platforms.