Athens Journal of Tourism - Volume 12, Issue 1, March 2025 – Pages 39-60

Privacy Concerns and Information Security in E-Tourism: Business and Information Management Perspective. The Case for Touring Companies in South Africa

*By Nkosingiphile Trevor Mchunu**

The travel and tourism industry has, in recent years, been one of the fastest-growing industries that has been highly digitised. However, it has brought about the accumulation and storage of large volumes of consumer data that have become a matter of great concern in the context of privacy and security within the e-tourism system. The lack of adequate protection of this information by tourist companies has led to financial losses, legal liabilities, and several detrimental impacts on the company, including loss of customer confidence and a potential threat to the company's future existence. This paper aims to discuss the most important privacy and security threats that the e-tourism sector encounters. To do so, it uses the lenses of consumer behaviour, information management, and business strategy, thus incorporating insights from several disciplines. This paper is a qualitative literature review research. The study also aimed to identify practical measures implemented by e-tourism organisations to face these complex issues in practice. The research highlighted the benefits of using blockchain, biometrics, and privacy-aware technologies. These tools help secure data and manage third-party risks. They also build customer trust in e-tourism. The study identified key risks like data breaches and third-party vulnerabilities. It also noted growing customer concerns about data use and personalized strategies.

Keywords: *E-tourism, privacy, information security, data governance, cyber security, consumer trust.*

Introduction

In recent years, the development of IT technologies has affected the tourism sector and the way people travel and organise their trips. The availability of smartphone applications and accommodation-sharing programmes, combined with online travel booking sites, has enabled clients to make informed decisions like never before (Grigalashvili, 2022; Purwita & Subriadi, 2019). Also, the advancement in e-tourism has led to the gathering and safeguarding of vast amounts of consumers' data, including their financial information, travel experience, and personal information (Xiang et al., 2022). This is due to the fact that electronic tourism companies have to use this data to offer better services and differential pricing, hence the need to protect such information (Grigalashvili, 2023).

In the context of privacy and security, tourists and organisations that cater to their needs are exposed to numerous threats (Hamid et al., 2021). Consequences arising from data breaches and security failures in e-tourism enterprises are often severe. Furthermore, it can also lead to financial and legal risks and can also significantly

*Graduate Student, Durban University of Technology, South Africa.

https://doi.org/10.30958/ajt.12-1-2 doi=10.30958/ajt.12-1-2

damage the company's image. Hence, there are long-lasting negative effects that could accrue from consumer trust breakdown (Xiang et al., 2022). Customers are at risk of being vulnerable to identity theft, fraud, and unauthorised usage of their information. According to Lama et al. (2020), these hazards can severely affect people in their day-to-day lives, including their digital security and financial health. All the e-tourism business has to solve these complex issues as a matter of great and immediate importance.

Tourism specialists have emphasised the importance of having a holistic and multi-disciplinary approach to the issues associated with privacy and security in the context of digital tourism (Hamid et al., 2021; Xiang et al., 2022). It is crucial to identify the problems that occur in the e-tourism area due to the fact that the effective management of information is critical for the formulation of strategic business decisions. Therefore, it is important to consider the various factors that may influence the e-tourism experience in the operational, technological and behavioural contexts (Lama et al., 2020; Mohammed et al., 2023). Thus, e-tourism enterprises need to build a proper balance of the possible usage of the client data for the improvement of the given services and the protection of the client's data (Pierdicca et al., 2019). The articulation of a legal framework for data management and the codification of measures for the security of data and rules for the use of data is to promote these requirements.

Complexity in the e-tourism information management problems is also a major factor. Some of the techs that are rising-face are (seamless integration of several data systems), risk management of third-party service providers and implementation of privacy-specific tech (Li et al., 2024). Consumers should be more protected in terms of personal data and give them more control over the information they share with e-tourism platforms. Additionally, they must ensure that security and compliance measures are strictly maintained throughout the entire value chain (Li et al., 2023). Innocence of these information security risks may result in system compromise, unauthorised access to data, and loss of consumers' confidence.

It is crucial to understand the relationship between the strategic management of organisations, information technology and consumer behaviour to ensure optimal management of privacy and security in e-tourism. This has been highlighted in the previous research works, which have been discussed earlier in this study (Hamid et al., 2021; Xiang et al., 2022). In the modern world, employees in the tourism industry may create effective measures to protect crucial information of customers, minimise possible risks, and gain the trust of tourists. This can be done by merging the information from different fields of study (Grigalashvili, 2022; Grigalashvili, 2023).

With this in mind, this research work seeks to examine the threat to the privacy and security of the e-tourism sector with a especial focus on information and business management. The literature on potential threats within the e-tourism sector and the primary findings reveal the most substantial risks in the given area, methods to minimise the impact of risks, and the role of modern technologies in improving data security and privacy concerns. This study will be useful for legislators, tourism organisations, and other actors who seek information about and action on the link between digitisation, consumer trust, and data protection in the tourism industry.

Whilst the prior research has focused on the security and privacy concerns within e-tourism from distinct standpoints, there happens to be a lack of an approach which combines consumer behaviour, information management, and the concept of business strategy. The study seeks to address the gap mentioned above by providing a holistic framework to explore to interplay that exists between the factors mentioned above in a bid to shape security and privacy issues within the ecosystem of e-tourism. As a result of the range of insights emanating from various disciplines, the research aims to offer a clear understanding of the issues and provide practical suggestions which can help to guide the organisations in e-tourism, the consumers and the policymakers to navigate the digital landscape at the same time protecting trust and ensuring the protection of data. The study also highlights the potential of emerging technologies like biometrics and blockchain in a bid to address the impending issues contributing to a continued narrative to leverage innovation to improve security and privacy in the concept of e-tourism.

Research Objectives

- To explore the regulatory compliance and the data practices of online travel organisations in line with security and privacy.
- To determine the security concerns in mobile applications and travel websites.
- To apprehend the protective behaviours and privacy concerns of online travellers.
- To identify the best practices and technical solutions in enhancing security and privacy within e-tourism

Literature Review

Using the guidelines given by Cooper et al. (2018) and Randolph (2019), a systematic literature review was conducted by the researcher. In this process, an initial search, and the screening process included the identification of the appropriate peer-reviewed articles, industrial reports, journals, and literature which is related to security and privacy issues within the e-tourism industry. The studies which were chosen were reviewed to find the challenges, risks, and recommendations in line with the processes of the collection of data, its storage, and the management practices in the context of e-tourism.

Data Collection and Storage by e-tourism Companies

Sensitive Customer Information at Risk

So, due to advancements in technology, particularly in the field of tourism, there are numerous online resources and platforms to arrange a trip, transportation, accommodation and even certain applications. These platforms give consumers information and choices which they can only get from these platforms (Henama & Apleni, 2020; Pierdicca et al., 2019). This is the case because travellers are using the e-tourism channels to access information for tourism purposes, make bookings

of travel products and services, and disclose personal details for travel. It encompasses their details such as their identification, contact information, booking and payment records, travel and tour information, and other information such as their passport numbers and information on the traveller's frequent flyer miles (Reverte & Luque, 2021; Xiang et al., 2022). Hence, the consumer data that e-tourism businesses gather to enhance their services, prices and promotions that are sent to consumers is vital in the current digital economy setting (Li et al., 2023; Reverte & Luque, 2021).

According to Al-Saad and Gharaibeh (2023), e-tourism companies posed a threat to consumers' privacy and data when they acquired and archived information from them. Chauhan and Singh (2020) observed that through hacking, data breaches, or any other security incident, the personal data of the traveller may be compromised. This can lead to consumers losing their identities, having their money misused and other negative consequences that can affect the consumers. Moreover, the effects that such incidents have on the business's reputation and the legal implications that are associated with such incidences are likely to cause damage to the trust that is at the center of the e-tourism environment and therefore harm the business.

For example, a number of e-tourism businesses have had challenges with the most appropriate ways of exploiting the customer's data in order to improve the customer's experiences while at the same ensuring that the customer's data is well protected from theft or misuse (Abdullahi et al., 2021). That is despite the fact that these privacy and security issues are critical. Due to poor data management and protection, the use of outdated security measures, and the lack of transparency in the way data is collected and used, travellers have been exposed, and this has led to their loss of confidence in online services for tourism (Reverte & Luque, 2021). Having identified these core challenges in the area of privacy and security of e-tourism, other stakeholders in the tourism industry, policymakers and other stakeholders have been forced to focus on these challenges as the environment for e-tourism continues to develop.

Potential Consequences of Data Breaches and Security Failures

According to Xiang et al. (2022) and Li et al. (2023), the vulnerability of the tourism industry to data breaches, cyberattacks, and other security failures, given the growing use of e-tourism platforms and dependence on technology. When such cases arise, the consequences can be dire as they will affect not only the tourism enterprises but the clients of these enterprises as well (Lama et al., 2020). As identified by Xiang et al. (2022) and Li et al. (2023), sanctions, legal consequences, and the costs of mitigation measures can burden or even harm an organisation financially. The decline in consumer trust results in a loss of market share, low customer retention, and a decline in the image of the brand. In severe cases, special security breaches have led to the shutdown of tourism companies as a consequence of their failure. This is because the affected firms' clients have switched their allegiance to more credible competitors (Al-Saad & Gharaibeh, 2023; Reverte & Luque, 2021).

However, besides the direct influence these have on enterprises which are involved in tourism, data breaches and security incidents that occur in the scope of e-tourism also pose certain threats to individual tourists. Cybercrimes like identity theft, financial fraud, and other related issues can greatly affect the consumer for a

long time (Abdullahi et al., 2021; Xiang et al., 2022). These crimes can happen when information that is personal and sensitive is revealed, including names, contact information, and payment card details, as well as passport information. The victims are struggling to reclaim control over their data and protect their online identity from further harm, and such cases can be psychologically and economically detrimental (Al-Saad & Gharaibeh, 2023; Hamid et al., 2021). It is also crucial to consider the financial aspect, which may also be an issue at times.

There has been significant concern about the use of consumer data within the e-tourism ecosystem and the possibility of abuse, which is a concern of privacy and data ethics (Lama et al., 2020; Reverte & Luque, 2021). Among the emerging challenges in the application of advanced analytics and personalisation algorithms in tourism businesses to deliver individual experiences, there are concerns that travellers' data is being tracked, profiled and monetised wrongly. These practices can be considered unethical and may result in violating the rights of individuals to privacy and also lose the confidence of consumers in the tourism industry (Abdullahi et al., 2021; Al-Saad & Gharaibeh, 2023). In the sphere of the e-tourism business, those numerous and complex problems have been identified and appear to be extremely essential for solving. This requires a comprehensive and cross-disciplinary approach and a careful balance between the opportunities offered by digitisation and the efforts to protect the privacy and security of clients.

Complex Tourism Supply Chains and Third-Party Risks

Distributed Data Systems and Access Control Challenges

This paper will, therefore, seek to paint a picture of the tourism business by understanding its structure, which has a complex and much-divided supply chain. These services are airlines, hotels, tour operators, travel agents and others to come up with a travel product (O'Connor, 2020). For the same reason that e-tourism platforms collect and exchange information with other third parties to provide consumers with a seamless process of booking and planning their trip, this ecosystem has become even more integrated in the digital age.

This distributed and integrated system of providing tourism services seems to have favoured the travellers in terms of time and specificity of service delivery but has posed some challenges of privacy and security that are quite complicated for the small e-tourism businesses to solve on their own (Reverte & Luque, 2021). It is a large tourism supply chain, and each supplier in this chain has its own way of managing and storing data, implementing security measures, and meeting standards (Cha et al., 2018). These providers usually acquire, store, and transmit information concerning the travellers, including their payment information. Suitable measures that include proper access control, secure handling of data transfer, and proper third-party management must be adopted to ensure adequate protection of such information in a fragmented and decentralised environment.

However, there are hundreds of thousands of tourism service providers, from large complex organisations to very small sensitive organisations and that is why the issue of the security situation becomes even more complex. This is because the threats and vulnerabilities that are present in one partner's systems can spread to the

other partner's systems and the entire e-tourism value chain and make it prone to risks and attacks (Lama et al., 2020). This means that the entire value chain is threatened, and the information of travellers can be compromised since each of the players in the tourism industry has weak cyber security measures, outdated software and poor access control systems, as seen among the smaller players in the value chain (Li et al., 2023).

Ensuring End-to-end Security and Compliance

Due to the increased coupling and the interdependencies of the e-tourism ecosystem on third-party services, the issue of offering a holistic, end-to-end security and compliance solution has become critical for organisations operating in the tourism sector (Hamid et al., 2021). However, attaining this level of comprehensive security and compliance is complicated because it implies integrating a number of actors whose data management systems, security measures and compliance policies are different. This is done so as to ensure that customer information is well protected and that there are no lapses in the protection of such information (Hamid et al., 2021). To avoid these risks, businesses that engage in e-tourism must ensure that they carry out thorough background checks on their third-party partners. This involves evaluating their standard security measures, management of cybersecurity incidents, and adherence to the law (Abdullahi et al., 2021). Furthermore, they are mandated to put in place clear contractual obligations that define the roles of the suppliers, service level agreements as well as ways to conduct ongoing monitoring so that the suppliers can be held to account and to ensure that there is continual oversight of the entire tourist system (Purwita & Subriadi, 2019).

Due to this, e-tourism companies face challenges in the process of identifying compliance needs within the security legal framework. This is because there is a need for them to meet their business operations and financial needs as well as the need to safeguard consumer information (Lin et al., 2020). As seen in the examples of data breaches, privacy violations, and regulatory non-compliance, the consequences include fines, customers 'switching to competitors, and trust loss, which are detrimental to the company's long-term performance (Hamid et al., 2021). Non-compliance with these regulations poses serious legal and reputational risks to these businesses and can lead to legal and reputational damages. To meet these challenges, it is thus essential for tourist businesses to be able to manage end-to-end security and compliance effectively in the context of the complex and increasingly interconnected digital environment. The e-tourism industry is still growing and developing (Lama et al., 2020).

Traveler Privacy Concerns and Expectations

Worries about Personal Data Usage and Profiling

Technological advancements such as e-tourism platforms, mobile applications, and other digital interfaces have enhanced the experience of travellers because they have access to more information and choices. While e-tourism firms are leveraging big data, artificial intelligence, and other targeted marketing approaches to offer enhanced individualised experiences, consumers are becoming more sensitive to the

potential risks of being monitored, profiled, and exploited by firms that engage in data tracking and profiling (Chauhan & Singh, 2020; Purwita & Subriadi, 2019).

While using the services of e-tourism providers, travellers often have to surrender rather sensitive information such as their names and contact information, payment information, travelling preferences and even location data (Xiang et al., 2022). Hamid et al. (2021) note that the unauthorised access, misuse, or sale of this personal data may lead to the occurrence of the following unfortunate events. Some of the activities are financial fraud, identity theft, target advertising, and invasive surveillance operations. There are growing worries about the impact on personal freedom and the violation of basic privacy rights as these data could be used to build comprehensive profiles of individual travellers' travelling patterns, preferences, and movements (Abdullahi et al., 2021).

Therefore, the majority of travellers have become rather cautious when it comes to e-tourism platforms because they are not quite sure about the possible risks of sharing their information with digital service providers (Li et al., 2024). This is because they are always afraid of what might happen if they are unable to get their information back. The decline of consumer confidence is an authentic issue that can affect the tourism industry (Li et al., 2023; Purwita & Subriadi, 2019). This is due to the fact that travellers may choose not to use the e-tourism services which offer ease and individual attention in favour of conventional offline methods of booking. Alternatively, they may decide not to travel at all to ensure that they do not expose themselves to the public and give away their information. Businesses that are into e-tourism have, therefore, had to grapple with the increasing concern that travellers have about the safety and use of their information. This calls for a comprehensive strategy that is informed by the benefits of personalisation while, at the same time, working to safeguard the rights of people.

Balancing Privacy with Personalised Services

Thanks to e-tourism, tourism businesses are capable of using a large amount of data about customers to offer them more individual attention and better services, variable pricing, and advertising. These aspects are vital in maintaining market competitiveness in the digital age (Clarke, 2021; Miao et al., 2019). As stated by Reverte and Luque (2021), e-tourism platforms can adjust the experience based on users' search histories, bookings, and preferences. This also helps the platforms to be able to make recommendations, offers, and bookings to the passengers, thus making them satisfied and loyal to the platforms.

As stated by Abdullahi et al. (2021), the enhanced level of personalisation comes at the cost of customer data collection, storage, and analysis, which is rather sensitive. This collection, storage and analysis of customers' data have generated much concern among many travellers with regard to their privacy. People gradually realise that their information, including their name, contacts, financial details, and travel history, may be misused, mishandled, or shared without their consent (Lama et al., 2020; Li et al., 2024).

Thus, due to this erosion of trust, the users may decide not to use the services of the digital platforms at all, or at least not to book their travels through these platforms and turn to the more traditional off-line ways of booking and travelling,

which may also mean not travelling at all (Gong & Schroeder, 2022). This can have severe consequences for the companies that are engaged in the e-tourism business. E-tourism, like any other online platform, faces the challenge of achieving the right balance between the righteous use of personalisation and respect for user privacy (Clarke, 2021). As suggested by Li et al. (2024), companies in the tourism sector must come up with strategies for the use of customer data that enhance the user experience and yet can guarantee the privacy of the individual and hence gain customer confidence.

As cited by Li et al. (2023) and Purwita and Subriadi (2019), some measures could be data management policies, privacy policies and simple means through which passengers can control data capture and usage. Moreover, tools like differential privacy and data anonymisation can help e-tourism companies offer services that are relevant to specific consumers without the danger of divulging their information (Abdullahi et al., 2021; Hamid et al., 2021). Thus, it will allow us to avoid the usage of data-driven personalisation for the e-tourism companies' aims in a way that can be unethical and can violate the customer's privacy rights. This is a critical assumption in the attainment of the long-term objectives of the industry and its prospects.

Methodology

Research Approach and Data Collection Methods

This study was founded in the systematic literature review as a significant possibility of summarizing the existing knowledge about the aspects of privacy and security of tourism and electronic tourism. Data collection and data materials in this research were developed according to the guidelines of Randolph (2019). It included several crucial steps.

An initial search in the Google Scholar database was run with terms such as 'privacy AND security AND e-tourism', 'data protection and online travel' and 'cybersecurity and travel websites'. The result was a search that brought up a significant amount of potentially relevant publications. Under the heading of filtering and appraisal, only the peer-reviewed and English-language published articles within the 2015-2023 period were regarded for further consideration by the researcher (Cooper et al., 2018). In addition, the abstracts and titles were assessed and reviewed in a bid to exclude the research within which security, privacy, and the protection of data concerns of the online travel providers or visitors were not addressed explicitly.

After rigorous, careful assessment, a final set of 67 highly relevant publications was retrieved. In order to avoid missing any other relevant works that the original searches might not capture, we rigorously conducted backward snowballing using the reference lists of the 67 publications, as suggested by Snyder (2019). Furthermore, some of the white papers, industry reports and other grey literature coming from authoritative sources were also provided to understand actual applications in real-world contexts. The introduction of these supplementary sources increased the value of academic literature, for the documents helped to examine actual problems in

privacy and security faced by e-tourism organisations and the tactics they used to prevent such threats (Paul & Criado, 2020).

Analytical Framework for Examining Privacy and Security in e-tourism

As argued by Paul and Criado (2020), the literature review approach allows for the construction of a theoretical framework that is multi-disciplinary for an understanding of security and privacy within the e-tourism sector. Such a framework draws upon perspectives in the disciplines of consumer behaviour, marketing, information systems and strategic management. The research concept and techniques followed the highest standards recommended both by academic literature and by industry.

From a strategic management perspective, the framework attempts to research how e-tourism organisations can benefit consumers' data by offering them personalized services and, at the same time, increasing their operational efficiency, data management, protection, and regulation compliance. It assesses the lack of well-defined policies for preventing data breaches and security infractions. The information management component of e-tourism systems leads to technological and operational issues, which relate to data integration problems, risks of using a third-party service provider, and approaches to improving data privacy.

This paradigm examines the methods by which e-tourism platforms might establish and enforce policies while still enabling consumer privacy and control. The consumer behaviour element examines the apprehensions of individuals who use the internet for travel purposes regarding the protection of their personal information and the level of security provided. It delves into their willingness to disclose personal information and trade-off of privacy for better services. Wong (2020) looks at consumer trust issues in e-commerce tourism platforms, the impact of privacy and security breaches on tourist behaviour, and the strategies to enhance consumer data privacy.

The research developed a broad, cross-disciplinary theoretical framework, applying diverse perspectives from corporate strategy, information management, and consumer behaviour better to understand the complex e-tourism environment of privacy and security. In particular, by synthesising previous research findings, this study provided practical and valuable implications and recommendations for many tourism stakeholders, including managers, IT professionals, legislators, and customers.

Central to this framework are three key constructs. The first is consumer behavior, which focuses on travelers' privacy concerns and their impact on trust and decision-making. Research highlights the privacy-personalization paradox, where consumers desire tailored experiences but fear data misuse (Clarke, 2021; Abdullahi et al., 2021). Understanding this trade-off is essential for analyzing consumer trust dynamics in e-tourism. The second construct, information management, examines operational and technological challenges, such as data governance and third-party risks. Effective data security practices, including encryption and anonymization, are critical to safeguarding consumer information and maintaining compliance with regulatory frameworks like GDPR (Li et al., 2023; Xiang et al., 2022). The third construct,

business strategy, addresses how organizations balance operational efficiency with ethical data practices. This involves leveraging data responsibly to enhance personalization while adhering to privacy standards to retain customer confidence (Grigalashvili, 2022).

The theoretical foundation builds on existing theories to inform the study's analysis. The privacy-personalization paradox offers insights into consumer preferences and hesitations in sharing personal data. Information management frameworks provide tools for analyzing data protection strategies, including end-to-end encryption and third-party audits, which are vital in the interconnected e-tourism value chain (Hamid et al., 2021). Business strategy theories, such as strategic resource management, evaluate how firms optimize data use to enhance service delivery without compromising trust (Li et al., 2023). These theories are particularly relevant in addressing challenges unique to e-tourism, such as fragmented supply chains and varied compliance standards across regions.

This study adopts an integrative theoretical lens, combining insights from the aforementioned frameworks to provide a robust approach to the research problem. The integration of these theories ensures that consumer concerns, organizational practices, and strategic imperatives are analyzed holistically. This alignment supports the study's goal of offering practical, interdisciplinary solutions to privacy and security challenges in e-tourism.

The application of this framework informs the research methodology by aligning theoretical constructs with the study's qualitative approach. For instance, consumer behavior insights guide the exploration of traveler privacy concerns, while information management theories inform the evaluation of organizational practices and technological solutions. Business strategy concepts underpin the analysis of how e-tourism firms implement privacy-focused strategies to maintain trust. This framework contributes to theoretical advancement by contextualizing established concepts within the e-tourism sector. By integrating these perspectives, the study addresses gaps in understanding how privacy and security issues intersect with operational and strategic priorities.

Findings

Theme 1: Regulatory Compliance and Data Practices

This can be seen in the modern world, especially in e-tourism, where businesses in the tourism sector have adopted the use of digital technologies and data analysis for personalisation and, therefore, face the challenge of privacy and data protection (Wong, 2020). If companies share the customers' information and it is not protected, they could face financial, legal and reputational risks, such as loss of the customer, which damages the future of the company (Grigalashvili, 2023).

Data Governance and Security Best Practices for e-tourism Firms

Robust Access Controls and Authentication

To reduce the likelihood of data leakage or misuse by clients, e-tourism companies should take strict measures in access control and the use of proper authentication (Wong, 2020). This involves the use of two or more factors, including passwords and biometric identification, as a way of validating users in order to access important information or perform important business activities (Xiang et al., 2022). However, e-tourism companies should also adhere to the principle of least privileging, which entails that the employee and third-party service providers should be given only the level of access necessary to perform their tasks. It is also crucial to examine these permissions from time to time and alter them in accordance with the organisation's needs and security policies whenever it is necessary (Hamid et al., 2021).

The processes of encryption, anonymisation, and data minimisation. Apart from access control, e-tourism firms have to ensure proper protection of data in order to safeguard the information that customers provide during business (Abdullahi et al., 2021). This means that encryption will be employed to guarantee that client data is not easily copied and used by unauthorised individuals during transmission and storage, and in the event that the data is exposed, it will be in an encrypted format that cannot be easily decrypted by anyone (Mohammed et al., 2023).

Besides encryption, other precautions that can be recommended for e-tourism organisations to strengthen consumer privacy protection are data anonymisation and data minimisation (Abdullahi et al., 2021). The information gathered from the customers can be useful to the business in its activities, but at the same time, the privacy of the customers must be preserved by deleting their information from the data set, as stated by Wong (2020). Other measures that should be put in place include data minimisation, where only information that is relevant to business activities should be collected and stored from customers to avoid data breaches and cyber-attacks (Hamid et al., 2021).

Incident Response and Breach Notification Protocols

Apart from implementing adequate measures for security, e-tourism firms should anticipate and be prepared to encounter data breaches or security incidents, as noted by Wong (2020). First, firms must establish proper incident response plans to allow them to detect, analyse, and respond to security breaches in the most appropriate and timely manner. This will help minimise the negative effects that may be experienced by the customers or the organisation (Abdullahi et al., 2021).

These incident response plans should outline the steps that should be taken to communicate the occurrence of a breach to the customers, regulatory authorities and other stakeholders. This increases the following of the code of ethics and other data protection laws and guidelines that are currently being used (Abdullahi et al., 2021). Furthermore, e-tourism businesses should periodically assess and modify their incident response plans. This should involve the incorporation of data from past occurrences as well as updating the current forms of threats. It can, therefore, assist in helping them build up their readiness to handle any other disasters that may occur in the future (Hamid et al., 2021).

Managing Third-party Risks in the Tourism Ecosystem

Vendor due Diligence and Security Assessments

Unfortunately, as e-tourism businesses have become more dependent on third-party service providers to deliver the products and services that they offer. It is imperative to address the concerns that may arise in the relationship with such entities (Xiang et al., 2022). Therefore, such examination, supervision, and control of these partnerships are called for.

These are the risks associated with third-party integration, and as such, e-tourism companies should ensure that they develop appropriate measures to ensure effective vendor selection and assessment of their security standards, as proposed by Lama et al. (2020). It is proposed to establish the existing cybersecurity level in the company, the possibility of dealing with incidents, the compliance with the legal framework before signing any contract's terms with any suppliers or companies engaged in business (Hamid et al., 2021). Similarly, the e-tourism companies should also assess from time to time the security that the current third-party partners present. This should include regularly checking and scanning, for example, auditing and pen testing, to check that these providers are still secure to use in the organisation (Wong, 2020).

Contractual Obligations and Service-level Agreements

In addition to the above steps, the identification of suitable contractual terms and SLAs between e-tourism companies and their third-party service providers can help in establishing a comprehensive strategy that ensures customer information security at every level of the supply chain (O'Connor, 2020). It should be clear from the provisions of the contract the kind of security measures that are expected, how incidents are to be handled and what actions are to be taken when there is a breach. However, they should also outline the roles of the e-tourism business and its third-party contractors in information protection (Lama et al., 2020).

With such contractual terms and service level agreements that have an emphasis on security, e-tourism companies are able to ensure that the third-party vendors are compelled to safeguard the data of the customers. This makes sure all the people involved understand the importance of safeguarding both the company and its consumers against any form of vices (Miao et al., 2019). Also, these contractual agreements can help the e-tourism businesses to set up certain measures and guidelines that have to be followed; any violation of which attracts legal consequences and also enables the e-tourism businesses to stop cooperation with third-party partners who may not meet the required standard of data protection as stated by (Cha et al., 2018).

Continuous Monitoring and Auditing of Third Parties

Apart from the initial check and legal requirements of the contract and agreement, e-tourism enterprises need to maintain continuous monitoring and auditing procedures to ensure that their third-party service providers will adhere to the necessary security and compliance standards in the future (Clarke, 2021). This involves checking on the security levels of these external partners, conducting periodic vulnerability assessments on their data protection practices, and looking out

This paper also notes that through the use of automated monitoring tools as well as security information and event management systems, there is a high possibility of enhancing the ability of the e-tourism enterprise to detect and respond to third-party security incidents in real time. This makes it easier to prevent harm and address legal issues arising from contracts and agreements and other legal relationships (Chauhan & Singh, 2020). Furthermore, e-tourism companies should also have clear steps for escalation and incident handling in case security issues are noticed in the e-tourism products and services. They should also be able to cut or alter relationships with third-party suppliers if they do not meet the required security level (Verhegghe, 2018).

Enhancing Customer Trust through Transparency and Control

Clear Data Privacy Policies and user Control Mechanisms

Besides enhancing internal data management and control and addressing risks related to third parties, e-tourism companies need to address the problem of trust in the eyes of their customers. This can be done by expanding the information on how data is utilised and permitting the consumers to have more control over their data (Sifolo & Henama, 2023). The first step is to develop simple-to-understand policies that define how the e-tourism company collects, stores and uses customers' information to prevent misuse as well as the safety measures put in place to protect the data (Verhegghe, 2018). It should outline the types of data that will be collected, the reason for collecting such data, and the measures that customers can take to access, correct or delete their personal information (Miao et al., 2019).

In addition, it is argued that the customers of e-tourism businesses must be able to exercise control over their data and the data that is being collected and used by e-tourism businesses by having the ability to select the data they want to share, the ability to In this way, e-tourism companies can ensure travellers' privacy and, therefore, gain their trust as well as distinguish themselves from the other companies in the highly competitive market.

Ethical Data Usage and Privacy-enhancing Technologies

Therefore, it becomes crucial that the e-tourism firms pay attention to the ethical use of data and try to adopt new techniques that would help increase the privacy of customers and, thus, increase the level of trust that the customers have in the system and support transparency. This will include observing the principles of data protection such as data minimisation whereby the only data that would be collected and stored from the customers would be the necessary one. It also encompasses ensuring that one does not engage in irresponsible or malicious use of data, including spying, tracking, or profiling of individuals or advertising (Clarke, 2021).

In addition, it is suggested that e-tourism companies should also consider employing advanced privacy-preserving measures, which include differential privacy, homomorphic encryption and secure multi-party computation. These strategies enable the organisation to get information from the customer data without infringing on the rights of the customers (Verhegghe, 2018). Therefore, with the integration of these modern technologies, e-tourism businesses will be in a better position to

practice ethical data management, recover customers' confidence, and set an example for other organisations in the correct utilisation of consumers' data (Cha et al., 2018).

Theme 2: The Security Concerns, Challenges and Emerging Solutions

The e-tourism sector has several crucial vulnerabilities in data protection and information security aspects (Clarke, 2021). In this regard, it is crucial to emphasise the importance of promoting the efficient use of technology to protect the customers' information, which will lead to the travellers' trust (Law & Chen, 2024). Some of the latest technologies, such as blockchain-based secure data sharing, biometric authentication, and privacy-preserving analytics, can be a powerful tool for e-tourism companies to overcome the challenges of security and privacy threats that are increasingly common in the digital world.

Blockchain is used for Secure Data sharing and Transaction Tracking

In this context, the distributed, decentralised architecture of blockchain technologies could be used to overcome the challenges related to data management and third-party risks within the e-tourism environment (Law & Chen, 2024). By tapping on the inherent features of blockchain, such as cryptographic data protection, irreversible transaction recordings, and consensus mechanisms, e-tourism

In the context of e-tourism, the most important application of blockchain technology is the secure exchange of client data, travel history, and booking transactions between the members of the decentralised network of tourism service providers. Furthermore, these systems provide a tamper-proof and immutable log of these interactions, which enhances their credibility (Paraskevas, 2022). This openness and accountability that has been realised and enhanced within the e-tourism industry can help not only in the early detection of security breaches but also in the identification of third-party partners who mishandle data (Vila et al., 2021).

Furthermore, the integration of blockchain technology and smart contracts can help in optimising compliance with contractual clauses and service level agreements that are focused on security and, thus, ensure that data protection laws are consistently applied across the entire e-tourism supply chain (O'Connor, 2020). Applying this approach, the process of managing risks related to third parties can be improved, the burden of compliance checking can be reduced and, thus, the confidence of e-tourism companies in their ability to protect the customers' data from all the partners in the ecosystem can be increased (Wong, 2020).

Biometrics for Robust Authentication and Access Control

In the e-tourism industry, biometric authentication technology and blockchain can enhance the security and privacy of customers (Xiang et al., 2022). Biometrics has embraced the use of unique physiological or behavioural characteristics such as fingerprint, face, and voice,, among others, to provide enhanced security and ease of identification as compared to conventional methods of using passwords. This technology assists in preventing the intrusions of unauthorised access to the customer data and the important e-tourism applications hence improving the aspect of security and privacy (Al-Saad & Gharaibeh, 2023).

Biometric identifiers cannot be easily forgotten or easily cracked compared to passwords, which may be easily guessed or shared. This makes biometric identifiers a viable option in protecting e-tourism businesses from traditional threats that include credential stuffing, phishing, and social engineering (Mohammed et al., 2023). Moreover, the biometrics may also be implemented alongside other forms of access control, such as multi-factor authentication and role-based access control, in order to give a more robust

Biometric technologies play a role in protecting e-tourism-related financial transactions alongside access control. The technologies assist travellers in confirming their identity when making payments or bookings through biometrics that are unique and unalterable to the individual (Reverte & Luque, 2021). This can, in turn, lead to increased customer satisfaction by enhancing the overall shopping experience and can also assist in reducing incidences of fraud and identity theft, a major issue of concern to consumers which may negatively affect the e-tourism websites (Grigalashvili, 2022).

Differential Privacy and other Privacy-enhancing Techniques

Differential privacy is a mathematical construct which allows for the sharing or utilisation of data while safeguarding the secrecy of the sensitive details that may be inferred from the data (Cha et al., 2018; Stadler et al., 2020). For instance, differential privacy mechanisms apply a fixed noise to the data and have a mathematical guarantee that it is impossible to couple the result of an analysis with an individual in the dataset. This protection remains active even when the level of difficulty is augmented by the selection of the opponent and background knowledge (Purwita & Subriadi, 2019). In e-tourism, it is crucial to implement the notion of privacy segmentation. From the above literature, it is evident that through consumer data analysis for personalisation and other purposes, business value can be created without violating the privacy of the travellers.

However, there are other possible technological solutions that e-tourism businesses should also consider as another method of safeguarding privacy; such as homomorphic encryption and Secure Multiparty Computation. This can also assist with improving the safeguarding of customer data while at the same time increasing the ease of access and value of the data (Miao et al., 2019; Stadler et al., 2020). When applied in e-tourism companies, such solutions enable the companies to show that they are concerned with the protection of consumers' data, and, therefore, the consumers will trust the companies and also set the bar for the proper handling of consumers' information (Stadler et al., 2020).

Some of the recent technologies that can also assist e-tourism organisations in combating the problems of data privacy and information security include blockchain, biometrics and privacy-preserving analytics (Miao et al., 2019). Therefore, the residents in this sector will be in a position to protect the data of their clients, prevent adverse incidents that may occur due to the involvement of other parties and, in the process, gain the trust of the tourists. These factors are very crucial for the e-tourism industry in order to manage and find ways to cope with the challenges which are present in the digital environment in order to make the industry sustainable and highly profitable in the future (Cha et al., 2018).

Theme 3: Traveler Privacy Concerns and Protective Behaviors

Key Privacy Concerns of Online Travelers

Many privacy threats for tourists in online interaction have also been detected by previous research, including unauthorised secondary application and mismanagement of personal data beyond what was declared; unauthorised access of sensitive data by third parties; mistakes in data collection and data oblivion that might lead to stress; and external data breach leading to identity theft as well as financial fraud (Abdullahi et al., 2021; Gong & Schroeder, 2022). Other notable research concerns disclosed travel information (dates, locations, and home address, among others which represents a safety issue when in the hands of criminals, traveller profiling for targeted advertising as invasive, and the sharing (lack of control and not knowing how the personal data is being used) of personal data with third-party affiliates (Paraskevas, 2022). Studies shown in interactive surveys highlight how IoT-enabled smart hotels (Berndt, 2022) are producing privacy leakages. In airline mobile apps, while the flight is on, real-time location and biometric data are also processed to show the location. Some new emerging technologies like VR, which can capture behavioural data, cost this privacy risk higher (Reverte & Luque, 2021).

Impact of Privacy Concerns on Traveler Behaviour

A high privacy concern might have a negative effect on the travellers' intention to perform online transactions, provide personal information and download mobile applications while going through the travel booking process (Vila et al., 2021). These concerns, especially around the risk of a potential impact, say from identity theft or data misuse, can be why an intended purchase is never made. When engaged in identity disclosure, the privacy and scam-threatened travellers intent to give up information or adopt completely new identities to conceal their private aspects, leading to incomplete information, false identification, or simply disappearing travellers instantly after putting data on the screen, undeniably affecting travel companies' conversions (Wong, 2020). The lack of explicit privacy guarantees on travel websites increases distrust and drop-off. As explained by Lin et al. (2020), travellers also appraise a site as untrustworthy when what they believe is an excessive amount of information is being collected, but they are not gaining equivalent value, such as being cautious about providing financial details.

Traveller Coping Strategies and Protective Behaviors

Research indicates that those who care about their privacy when they go online take precautions in terms of technology use, such as only using their browsers' privacy settings, checking if web pages are SSL encrypted, and putting on ad blockers, among others, including flight trackers so that they can have a say on many things while surfing (Law & Chen, 2024). Further, measures to be taken are to use anonymous browsing or partially or even wrongly completed personal details to escape identification and to avoid visiting travel websites and applications with excessive or extensive data gathering. Non-technical coping behaviours may include greater use of relatively privacy-preserving traditional offline booking channels or segmenting the information shared between different parts of the same travel website to avoid

extensive profiles being built up (Mohammed et al., 2023). Survey results also suggest that the travellers are unaware of existing tools and have difficulties understanding the long privacy policies, which shows a gap in the privacy provisions currently enforced.

Theme 4: Solutions and Best Practices for Privacy and Security

Regulatory Compliance and Data Governance Frameworks

Various regulations and frameworks are needed to promote consumer confidence and ensure proper, ethical, and secure treatment and management of the traveller data with consent requirements for collection/processing, the limitation of storage duration, and control of secondary usage (Al-Saad & Gharaibeh, 2023). Necessary regulations include the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and sector-specific data protection regulations for travel industry providers that entail restrictive opt-in mandates, mandatory breach disclosures, and heavy penalties for non-compliance. In a non-profit manner at the global level, the Travel Technology Data Governance Framework, for instance, offers certification for organisations following very high data privacy standards in respect of their use of data of customers by adhering to principles of integrity, necessity and access security (Henama & Apleni, 2020). Internal governance policies covering purpose limitation, retention schedules, access rights, and training can effectively manage privacy risks to empowerment.

Privacy-Enhancing Technologies and Cybersecurity Measures

Effective encryption techniques are used in stored travel data as well as transmission conduits to prevent unauthorized persons from accessing the information; thereby, personal privacy is maintained. Other emerging technologies include the use of tokenisation; hence, cardholders' sensitive payment card credentials are concealed while making a purchase online (Li et al., 2023). Other solutions encompass blockchain- based decentralized credential management, eliminating single-point security risks (Abdullahi et al., 2021). Artificial intelligence (AI) and machine learning (ML) models also allow predictive analysis to identify abnormal activities and automated threat responses. Privacy and federated analysis are examples of privacy-protecting technologies adding safety nets compared with simply identify-unlinking information extraction for data analysis. Additional cybersecurity measures can include preventing access control, auditing and penetration testing, secure coding in software development and ensuring that employees are well-trained in security awareness (Henama & Apleni, 2020).

Building Consumer Trust through Transparency and Control

Thus, it is imperative to adopt GDPR-enhanced strategies to enhance consumer trust and mitigate privacy issues within the travel industry. This translates to providing information on data collection and use, securing consent when the case applies for processing, and granting users the right to his/her data on e-platforms, such as to access and correct such data (O'Connor, 2020). Furthermore, designing the privacy control panels for visibility of the parts in the use of data and the guidance for making the preferences on non-essential tracking to promote the self-regulation ways of data

sharing with checkups and licenses could be useful for travellers (Wong, 2020). From the researched literature, therefore, it emerges that when people feel that they satisfy the characteristics of open information and have at least some degree of control over the information they input, they are able to choose that information as well as the trust to be placed in platforms.

Conclusion

The progress of the tourism sector has greatly improved the ways through which tourists plan their travel, identify the services they require, and how they navigate through the use of technological applications to get information and services. However, the shift to e-tourism has created a scenario where large amounts of clients' data are collected and stored, thus posing a threat to their privacy and security. The threats that exist in the e-tourism environment include breach of data, system failure and IP theft, and access of unauthorised persons to consumer data, which results in financial and non-financial losses, legal consequences, and business risks for organisations in the tourism industry. In addition, the structure of the supply chain of tourism, which includes several interconnected sub-chains and involves many third-party suppliers connected to the same information systems, has stimulated the emergence of new threats and risks that e-tourism companies should combat.

E-tourism, being a relatively new concept, is confronted with numerous operational and technological issues it has to address. At the same time, it has to address consumers' concerns on the protection of privacy, use of data, and personalisation. This means that if traveller's concerns are not met, the consumers may not trust e-tourism services and may switch to traditional services and products, which include the offline channels of booking.

Recommendations for E-tourism Organisations and the Industry

In order to mitigate the issues of privacy and security in e-tourism, there is a need for enterprises to adopt a holistic management approach that involves business strategy, information management and consumer behavior. For instance, to ensure that the customer information is secure and to prevent data breaches or security failure, e-tourism companies should adopt strong data governance measures such as Controls, Encryption, and Incident Management. At the same time, these businesses must identify third-party risks, conduct thorough due diligence, state contractual obligations, and periodically examine the cybersecurity policies of the partners in their ecosystem.

In addition to these operational and technological strategies, e-tourism companies should consider enhancing consumer confidence by adopting more transparent practices and implementing more user control features. Justifiable and simple data protection regulations, highly granular control over permissions and data management, and the adherence to generally accepted principles of data use that do not infringe on the rights of an individual. E-tourism businesses should adopt the use of emerging

technologies such as blockchain, biometrics, and privacy-enhancing analytics to enhance their privacy and security in light of the emerging challenges in the industry. Hence, the tourism organisations that opt for these enhanced solutions can enhance data protection measures, manage the risks from third-party vendors, and offer services that are tailored to consumers without compromising their privacy.

Thus, the actors in the correct handling of privacy and security in e-tourism include the tourism enterprises, the technology providers, the policymakers, and the consumer protection authorities. In this manner, the industry can create a pathway for establishing consumer confidence and work on its efficiency and correct data management in a way that is key for its growth and the improvement of travelling experiences in the digital age.

Limitation of the Study

The limitations of this study are tied to its reliance on a qualitative literature review, which may lack the robustness of empirical, data-driven methodologies. The results synthesize the available literature, which may not accurately capture fast-changing threats or technological solutions in e-tourism. It also limits variance related to regional nuances and stakeholder-specific perspecties within the ecosystem of e-tourims. Second, this focus on block chain, biometrics and privacy-enhancing technologies is forward -looking but dies not duly consider the challenges of their practical implementation or consumer acceptance barriers.

Future Research Directions

This paper has presented a case for the need to pay attention to issues of privacy and security in the e-tourism business as the field grows in the future; several avenues of research can be taken to advance further the knowledge and management of these concerns in this industry.

One of the key and important areas of research is the empirical analysis of the financial, operational, and reputational costs and consequences of data breaches and security incidents for e-tourism companies and the effects of such events on consumers' trust and behaviour in the future. This work can contribute to the development of better practices for managing risks and provide recommendations for investments in security technologies and data protection.

In addition, future studies should explore the effectiveness and readiness of future privacy-enhancing technologies such as blockchain, biometrics, and differential privacy for e-tourism applications. This may involve identifying the potential technical and operational risks and opportunities in implementing these novel solutions, understanding consumer attitudes and orientations towards these solutions, and evaluating the positive and negative effects of these solutions on the overall user experience and the capacity of the e-tourism industry to manage the tension between personalisation and privacy.

Legal frameworks and industry standards define the level of privacy and security within e-tourism firms. Academic research could also focus on the practical applicability of current legislation, such as the GDPR or CCPA, with regard to the specific

concerns of the tourism sector as well as possibilities for enhanced standardisation for compliance and consumer trust.

References

Abdullahi M, Kilili R, Günay T (2021) E-tourism and digital marketing in africa: opportunities and challenges. *Linguistica Antverpiensia*, *21*(1), 244-261.

Al-Saad S, Gharaibeh B (2023). E-tourism adoption in travel agencies: new qualitative insights from a developing country. *International Journal of Tourism Policy*, *13*(3), 248-261.

Berndt L (2022) *E-procurement for destination management companies within the tourism industry in South Africa: digital era trends, challenges and responses*

Cha S-C, Hsu T-Y, Xiang Y, Yeh K-H (2018) Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. *IEEE Internet of Things Journal*, *6*(2), 2159-2187.

Chauhan R, Singh D (2020) *Ensuring privacy-aware data release: an analysis of applicability of privacy enhancing techniques to real-world datasets*. 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),

Clarke R (2021) *An Intelligent Client-Centric Framework for Responsive, Privacy Conscious Personalisation* Trinity College].

Cooper C, Booth A, Varley-Campbell J, Britten N, Garside R (2018). Defining the process to literature searching in systematic reviews: a literature review of guidance and supporting studies. *BMC medical research methodology*, *18*, 1-14.

Gong Y, Schroeder A (2022) A systematic literature review of data privacy and security research on smart tourism. *Tourism Management Perspectives*, *44*, 101019.

Grigalashvili V (2022) E-government and E-governance: Various or Multifarious Concepts. *International Journal of Scientific and Management Research*, *5*(1), 183-196.

Grigalashvili V (2023) Digital Government and Digital Governance: Grand Concept. *International Journal of Scientific and Management Research*, *6*(2).

Hamid RA, Albahri AS, Alwan JK, Al-Qaysi Z, Albahri OS, Zaidan A, Alnoor A, Alamoodi, AH, Zaidan B (2021) How smart is e-tourism? A systematic review of smart tourism recommendation system applying data management. *Computer Science Review*, *39*, 100337.

Henama US, Apleni L (2020) The effect of E-Commerce travel agencies in East London, South Africa. *African Journal of Hospitality, Tourism and Leisure*, *9*(1), 1-14.

Lama S, Pradhan S, Shrestha A (2020) Exploration and implication of factors affecting e-tourism adoption in developing countries: a case of Nepal. *Information Technology & Tourism*, *22*(1), 5-32.

Law R, Chen S (2024). Developments and implications of tourism information technology: a horizon 2050 paper. *Tourism Review*.

Li F, Li H, Niu B (2024) Advances in Privacy Preservation Technologies. In *Privacy Computing: Theory and Technology* (pp. 17-42). Springer.

Li P, Zhou Y, Huang S (2023) Role of information technology in the development of e-tourism marketing: A contextual suggestion. *Economic Analysis and Policy*, *78*, 307-318.

Lin P-P, Li D-F, Jiang B-Q, Yu G-F, Wei A-P (2020) Evaluating the comprehensive impacts of tourism in Hainan by intergrating input-output model with MCDM methods. *Technological and Economic Development of Economy*, *26*(5), 989-1029.

Miao Q, Jing W, Song H (2019). Differential privacy–based location privacy enhancing in edge computing. *Concurrency and Computation: Practice and Experience*, *31*(8), e4735.

Mohammed R, Alamoodi A, Albahri O, Zaidan A, AlSattar H, Aickelin U, Albahri A, Zaidan B, Ismail AR, Malik R (2023) A decision modeling approach for smart e-tourism data management applications based on spherical fuzzy rough environment. *Applied Soft Computing*, *143*, 110297.

O'Connor P (2020) Data privacy and the travel sector. *Handbook of e-Tourism*, 1-14.

Paraskevas A (2022) Cybersecurity in travel and tourism: a risk-based approach. In *Handbook of e-Tourism* (pp. 1605-1628). Springer.

Paul J, Criado AR (2020) The art of writing literature review: What do we know and what do we need to know? *International business review*, *29*(4), 101717.

Pierdicca, R., Paolanti, M., & Frontoni, E. (2019). eTourism: ICT and its role for tourism management. *Journal of Hospitality and Tourism Technology*, *10*(1), 90-106.

Purwita AW, Subriadi AP (2019) Information technology investment: In search of the closest accurate method. *Procedia Computer Science*, *161*, 300-307.

Randolph J (2019) A guide to writing the dissertation literature review. *Practical assessment, research, and evaluation*, *14*(1), 13.

Reverte FG, Luque PD (2021) Digital divide in e-Tourism. In *Handbook of e-Tourism* (pp. 1-21). Springer.

Sifolo PPS, Henama US (2023) The role of governance in tourism planning. In *Handbook on Tourism Planning* (pp. 119-131). Edward Elgar Publishing.

Snyder H (2019) Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333-339.

Stadler W, Kalloniatis C, Travieso-Gonzalez C (2020) Risks of Privacy-Enhancing Technologies: Complexity and Implications of Differential Privacy in the Context of Cybercrime. *Security and Privacy From a Legal, Ethical, and Technical Perspective*, *9*.

Verhegghe P (2018) Personalization privacy paradox on facebook.

Vila TD, González EA, Vila NA, Brea JAF (2021) Indicators of website features in the user experience of e-tourism search and metasearch engines. *Journal of theoretical and applied electronic commerce research*, *16*(1), 18-36.

Wong AT-T (2020) E-TOURISM: HOW CUSTOMERS'INTENTION TO USE BE AFFECTED? *Academy of Marketing Studies Journal*, *24*(4), 1-19.

Xiang Z, Fuchs M, Gretzel U, Höpken W (2022) *Handbook of e-Tourism*. Springer.