Tourism Security and Cybercrime and Their Impact on The Arab Tourist

الأمن السياحي والجرائم الإلكترونية وتأثيرها على السائح العربي

DEHIMI Mohammed Tayeb
Laboratory of Mechanisms for Achieving Comprehensive Development in Algeria
Faculty of Law - University of Algiers 1
m.dehimi@univ-alger.dz

Date of Submission 07-01-2026 Date of Final Acceptance 25-05-2026 Date of Publication June 2026

Abstract:

This study examines the structural reconfiguration of tourism security in the context of digital transformation, with particular emphasis on cybercrime and its impact on the Arab tourist. As tourism increasingly operates within digital ecosystems, traditional security approaches focused on physical protection have become conceptually and practically inadequate. The research identifies a clear normative and institutional gap in Arab legal frameworks regarding cybersecurity, data protection, and digital trust in tourism governance. Adopting a comparative analytical methodology and drawing on international standards, the study analyzes the repercussions of cybercrime on tourist confidence and destination competitiveness, and proposes an integrated Arab model of smart tourism.

Keywords: Tourism Security; Cybercrime; Cybersecurity; Smart Tourism; Digital Trust.

ملخص:

تعالج هذه الدراسة إعادة تشكّل مفهوم الأمن السياحي في ظل التحول الرقمي، من خلال تحليل تأثير الجرائم الإلكترونية على السائح العربي. فمع اندماج السياحة في منظومات رقمية معقّدة، لم تعد المقاربات التقليدية للأمن السياحي، القائمة على الحماية الميدانية، قادرة على استيعاب طبيعة المخاطر المستجدة. وتكشف الدراسة عن فجوة معيارية ومؤسسية في التشريعات العربية، خاصة في مجالات الأمن السيبراني، وحماية البيانات، وبناء الثقة الرقمية. واعتمادًا على منهج تحليلي مقارن ومعايير دولية، تحلل الدراسة انعكاسات الجرائم الإلكترونية على ثقة السائح وتنافسية الوجهة السياحية، وتقترح نموذجًا عربيًا للأمن السياحي الذكي يقوم على الوقاية، والحوكمة، والاستباق.

الكلمات المفتاحية: الأمن السياحي؛ الجرائم الإلكترونية؛ السياحة الذكية؛ الأمن السيبراني؛ الثقة الرقمية.

*** Corresponding Author: DEHIMI Mohammed Tayeb**

Introduction:

The tourism sector has undergone profound transformations over the past two decades as a result of accelerated digitalization and the widespread integration of information and communication technologies into tourism activities. Tourism has progressively evolved into a complex digital ecosystem relying on online booking platforms, electronic payment systems, mobile applications, and interconnected information systems. While these developments have enhanced efficiency and accessibility, they have also generated new forms of vulnerability affecting both tourists and tourism institutions.

In this context, tourism security has emerged as a central concern for public authorities and tourism stakeholders. Traditionally associated with the protection of tourists against physical risks and conventional crimes, tourism security has expanded to encompass digital threats operating in virtual and transnational environments. This evolution reflects a fundamental shift in the nature of risks affecting tourism activities and calls for a reassessment of existing conceptual and legal frameworks.

The relevance of this study lies in the growing gap between the rapid digital transformation of tourism and the limited adaptation of legal and institutional frameworks designed to protect tourists, particularly in the Arab world. Despite the increasing reliance on digital tools throughout the travel cycle, tourism security policies in many Arab countries remain predominantly focused on traditional forms of protection, while cybersecurity, data protection, and digital trust are not yet fully integrated into tourism governance.

Against this background, the study is structured around the following central research problem: **To what extent are existing tourism security frameworks capable of adapting to the digital transformation of tourism and effectively protecting tourists from emerging cyber risks, particularly in the Arab context?**

This central question gives rise to the following sub-questions:

– How has the concept of tourism security evolved in response to digital transformation?

– What are the main forms of cybercrime affecting tourists within the tourism sector?

– What are the impacts of these cyber threats on the Arab tourist and on tourism destinations?

– What legal and institutional limitations affect the effectiveness of current tourism security frameworks?

– How can an integrated model of smart tourism security be developed to address these challenges?

The objective of this study is to analyze the transformation of tourism security in the digital era and to assess its implications for tourist protection, with a particular focus on the Arab context. To achieve this objective, the study examines the conceptual evolution of tourism security, analyzes the nature and forms of cybercrime affecting tourists, and evaluates their impacts, before exploring the legal and institutional conditions required to develop an integrated model of smart tourism security.

Methodologically, the study adopts a qualitative analytical approach based on doctrinal legal analysis and the examination of relevant regulatory frameworks and international standards. It focuses on observable legal and institutional realities in order to provide a coherent and structured assessment of tourism security challenges.

The scope of the study is limited to the analysis of tourism security in relation to cybercrime affecting tourists, with particular emphasis on the Arab region. This delimitation ensures analytical coherence and allows for the formulation of conclusions that are directly relevant to the regional context.

The study is structured into four main sections. **The first section** examines the concept and evolution of tourism security. **The second section** analyzes cybercrime in the tourism sector and its forms affecting tourists. **The third section** explores the impacts of these crimes on the Arab tourist and tourism destinations. **The fourth section** proposes a model of smart tourism security adapted to the Arab context.

Section I: The Concept and Evolution of Tourism Security.

Tourism security constitutes a fundamental dimension of tourism governance, as it directly affects the protection of tourists, the stability of tourism activities, and the overall attractiveness of destinations. Traditionally, tourism security has been closely associated with the broader notion of public security, and has been regarded as one of its functional extensions. In this sense, tourism security was primarily conceived as a mechanism aimed at protecting tourists from conventional criminal acts that might occur during their stay, such as theft, assault, fraud, or harassment, particularly in highly frequented tourist areas [1].

This traditional conception of tourism security emerged in a historical context in which tourism activities were predominantly physical in nature and geographically localized. Tourists interacted directly with service providers, moved within clearly identifiable spaces, and relied mainly on face-to-face transactions. As a result, security risks were perceived as visible, localized, and manageable through classical law enforcement tools. The role of the State was therefore centered on maintaining public order, ensuring police presence in tourist zones, and providing assistance and guidance to visitors, often through specialized tourist police units [2].

From a legal perspective, this approach was reflected in tourism legislation in many countries, including Arab States. Tourism laws focused mainly on administrative regulation, such as licensing tourism establishments, classifying hotels, regulating travel agencies, and organizing tourism professions. While these regulatory mechanisms contributed to structuring tourism activities, they rarely addressed tourism security as an autonomous legal concept or provided explicit provisions for the protection of tourists against emerging risks[3]. Consequently, tourism security remained implicit rather than codified, and was treated as an operational issue rather than a comprehensive legal and institutional framework.

This traditional model of tourism security is characterized by its reactive nature. Security intervention generally occurs after an incident has taken place, with limited emphasis on prevention, risk anticipation, or systemic vulnerability assessment. While such an approach proved relatively effective in addressing localized and visible threats, it revealed significant limitations as tourism activities became more complex and interconnected. The expansion of tourism flows, the diversification of services, and the increasing involvement of private actors exposed the inadequacy of a security model focused exclusively on physical protection [4].

The limitations of the traditional approach became even more evident with the gradual integration of technology into tourism services. The emergence of electronic booking systems, online travel agencies, and digital payment tools transformed tourism into a partially dematerialized activity, extending security risks beyond physical spaces. However, in many Arab countries, tourism security strategies continued to rely on field-based measures and policing, while economic security, health security, and digital protection remained marginal or insufficiently integrated into tourism policy [5].

In response to these transformations, tourism security has progressively evolved toward a more comprehensive and multidimensional concept. Contemporary approaches emphasize the need to integrate physical security with cybersecurity, data protection, health risk management, and trust-based mechanisms. This evolution reflects a broader understanding of security as a governance issue rather than a purely operational function. Tourism security is now increasingly perceived as a prerequisite for sustainable tourism development, destination competitiveness, and the preservation of tourists' confidence in an increasingly digitalized environment [6].

This section is structured into two main parts. The first examines the traditional concept of tourism security, while the second analyzes its transformation toward a comprehensive and digital approach.

A) The Traditional Concept of Tourism Security:

The traditional concept of tourism security is rooted in classical theories of public security and crime prevention. It focuses primarily on protecting tourists from direct physical harm and maintaining order in tourist areas through visible security measures. This approach prioritizes deterrence, surveillance, and rapid intervention, relying heavily on police presence and administrative control mechanisms.

Within this framework, the protection of tourists is largely dependent on the capacity of law enforcement agencies to respond to incidents, rather than on proactive risk management. Legal provisions tend to emphasize sanctions and enforcement, while preventive strategies and coordination with other sectors remain limited. Although this model continues to play an important role in ensuring basic safety, its scope remains insufficient to address the complexity of contemporary tourism risks.

B) The Transformation toward Comprehensive and Digital Tourism Security:

The transformation of tourism security reflects the broader digital shift affecting tourism activities. As tourism services increasingly rely on digital platforms and data-driven systems, security risks have expanded to include cyber threats, data breaches, and digital fraud. This evolution requires a redefinition of tourism security that integrates legal, institutional, and technological dimensions.

Comprehensive tourism security is therefore based on coordination between multiple actors, including tourism authorities, cybersecurity agencies, law enforcement bodies, and private sector stakeholders. It emphasizes prevention, anticipation, and resilience, rather than mere reaction. This transformation marks a decisive shift toward a governance-based model of tourism security capable of addressing both traditional and digital threats in a coherent and sustainable manner.

The analysis of the concept and evolution of tourism security highlights a fundamental shift in the understanding of security within the tourism sector. The traditional model, rooted in physical protection and public order maintenance, was closely aligned with the historical characteristics of tourism as a localized and predominantly physical activity. While this model remains relevant for addressing visible and immediate threats, it proves insufficient when confronted with the structural transformations brought about by digitalization and globalization[7]

The evolution toward comprehensive tourism security reflects the growing complexity of tourism systems and the diversification of risks affecting tourists. Security is no longer limited to preventing physical harm, but now encompasses digital protection, data security, health risk management, and trust-based mechanisms. This transformation underscores the necessity of redefining tourism security as a governance issue that integrates legal, institutional, and technological dimensions, rather than as a purely operational function. Such reconceptualization constitutes the theoretical foundation upon which contemporary tourism security strategies must be built [8].

Section II: Conceptual and Legal Framework of Cybercrime in the Tourism Sector

The growing dependence of tourism activities on digital technologies has fundamentally altered the risk environment surrounding tourism. The expansion of online booking platforms, electronic payment systems, mobile travel applications, and digital communication tools has transformed tourism into a data-intensive sector, making it particularly vulnerable to cybercrime. Unlike traditional security threats, cybercrime operates in virtual spaces that transcend territorial borders, rendering conventional security mechanisms insufficient. As a result, cybercrime has emerged as a central challenge to contemporary tourism security, particularly in regions where legal and institutional frameworks have not kept pace with digital transformation [9].

These challenges are further reinforced by the transnational nature of cybercrime, which operates across multiple jurisdictions and often exceeds the regulatory capacity of individual States. As a

result, the vulnerabilities identified in this section cannot be fully addressed within purely national frameworks. This highlights the structural limits of existing responses and underscores the need for more coordinated and integrated approaches.

In the Arab context, the impact of cybercrime on tourists is amplified by structural factors such as uneven levels of digital infrastructure, limited cybersecurity awareness, and the absence of sector-specific legal protections for tourists engaging in digital travel transactions. Arab tourists increasingly rely on digital tools to plan, book, and manage their trips, often interacting with foreign platforms subject to complex jurisdictional regimes. This reality raises serious questions about the capacity of existing tourism security systems to protect tourists from digital risks and ensure effective remedies in cases of cyber incidents [10].

This section is structured into three parts. The first defines cybercrime in the tourism sector, the second analyzes its main forms, and the third examines the legal dimensions and structural vulnerabilities that characterize cybercrime in tourism-related digital environments.

A) The Concept of Cybercrime in the Tourism Sector :

Cybercrime in the tourism sector refers to all unlawful acts committed through information and communication technologies that directly or indirectly target tourists, tourism institutions, or tourism-related digital platforms. These crimes include, but are not limited to, online fraud, identity theft, hacking of databases, phishing attacks, and the manipulation of digital booking systems. What distinguishes cybercrime in tourism from other forms of cybercrime is its close connection to personal mobility, financial transactions, and the exchange of highly sensitive personal data [11].

The transnational nature of tourism-related cybercrime constitutes one of its defining characteristics. Cybercriminals often operate across multiple jurisdictions, exploiting legal gaps and enforcement limitations. This makes detection, investigation, and prosecution particularly complex, especially when tourists are victims of crimes committed through platforms located outside their home countries or the destination State. As a result, cybercrime in tourism challenges traditional legal notions of jurisdiction, responsibility, and accountability [12].

Furthermore, the tourism sector's reliance on multiple interconnected actors—hotels, airlines, travel agencies, booking platforms, and payment service providers—creates a fragmented digital ecosystem with numerous points of vulnerability. Each actor processes and stores tourist data, increasing the risk of unauthorized access, data leakage, and misuse. This structural complexity makes tourism an attractive target for cybercriminals and heightens the exposure of tourists to digital threats throughout the travel cycle [13].

From a legal standpoint, cybercrime is generally defined as any unlawful act committed through information and communication technologies, targeting data, systems, or users. Although most national legislations do not provide a tourism-specific definition of cybercrime, general cybercrime frameworks apply fully to tourism-related digital activities. According to international practice, acts such as online fraud, identity theft, unauthorized access to databases, and manipulation of digital platforms fall within the scope of cybercrime when committed through electronic means [14].

In the tourism sector, the legal relevance of cybercrime is amplified by the nature of the data processed. Tourism institutions routinely collect sensitive personal data, including passport details, payment information, travel itineraries, and accommodation records. Under contemporary legal standards, such data enjoy enhanced protection due to their potential misuse and the significant harm that may result from security breaches. Consequently, cybercrimes targeting tourism platforms constitute not only economic offenses but also violations of privacy and consumer protection norms [15].

This legal framing demonstrates that cybercrime affecting tourists must be addressed through an integrated application of cybercrime law, data protection law, and consumer protection law, rather than through isolated criminal provisions.

B) Forms of Cybercrime Targeting Tourists:

Cybercrimes targeting tourists take diverse forms, reflecting the multiplicity of digital services involved in tourism activities. One of the most widespread forms is online booking fraud, whereby fake websites or fraudulent platforms offer deceptive travel services, accommodation, or airline tickets at seemingly attractive prices. Tourists often discover the fraud only upon arrival at the destination or when attempting to use the purchased service, resulting in financial loss and psychological distress.

Another prevalent form of cybercrime involves the theft of personal and financial data through hacking or phishing attacks. Cybercriminals exploit unsecured hotel databases, compromised Wi-Fi networks, or malicious links sent via email and messaging applications to obtain sensitive information such as passport details, credit card numbers, and travel itineraries. This data may then be used for identity theft, financial fraud, or illegal resale, extending the harm far beyond the initial travel experience[16] .

Cybercrime also affects tourism institutions directly, with indirect consequences for tourists. Ransomware attacks on hotel management systems or airline reservation platforms can disrupt services, lead to mass cancellations, and expose large volumes of customer data. Such incidents undermine trust in tourism institutions and highlight the interdependence between institutional cybersecurity and tourist protection.

C) Legal Dimensions and Structural Challenges of Cybercrime in Tourism

From a legal and structural perspective, cybercrime in the tourism sector cannot be reduced to isolated digital offenses or individual acts of fraud. The contemporary tourism industry operates through highly interconnected technological infrastructures that combine online booking systems, cloud-based databases, mobile applications, electronic payment gateways, biometric identification tools, and real-time communication networks. This increasing technological dependence has transformed tourism into a complex digital ecosystem in which vulnerabilities affecting a single actor may rapidly extend to multiple institutions and tourists simultaneously.

The structural complexity of this ecosystem creates significant cybersecurity challenges. Tourism operators often rely on interconnected third-party platforms and external service providers for reservations, payment processing, customer management, and data storage. As a result, security breaches may occur not only through direct attacks on tourism institutions, but also through weaknesses affecting subcontractors, cloud infrastructures, unsecured Wi-Fi networks, or poorly protected digital interfaces. This interdependence increases systemic vulnerability and complicates the identification of the source of cyber incidents.

From a legal standpoint, these technical realities generate complex issues relating to jurisdiction, liability, data governance, and regulatory coordination. Cyber incidents affecting tourists frequently involve cross-border digital transactions, foreign platforms, and multiple actors operating under different legal systems. Consequently, tourists may encounter considerable difficulties in identifying the responsible party, determining the applicable law, or obtaining effective remedies and compensation. The fragmented nature of legal regulation further aggravates these difficulties, particularly where tourism legislation, cybersecurity frameworks, consumer protection rules, and data protection laws operate independently from one another.

In addition, structural inequalities in digital infrastructure and cybersecurity capacities represent a major challenge in the Arab context. While some tourism destinations have adopted advanced digital

systems and cybersecurity mechanisms, others continue to face limitations related to technical resources, institutional coordination, cybersecurity awareness, and specialized expertise. These disparities weaken the resilience of tourism systems and increase tourists' exposure to digital risks.

These legal, technical, and structural challenges demonstrate that cybercrime in tourism is not merely a criminal or technological issue, but a broader governance challenge requiring integrated legal regulation, institutional coordination, technological resilience, and preventive security strategies. Such challenges also explain why the consequences of cybercrime extend beyond isolated incidents and directly affect tourist confidence, destination image, and the sustainability of tourism development.

These legal, technical, and structural vulnerabilities provide the analytical foundation for examining, in the following section, the multidimensional impact of cybercrime on Arab tourists, digital trust, and destination competitiveness.

Section III: The Impact of Tourism Cybercrime on Arab Tourists and Destination Trust

The analysis of cybercrime in the tourism sector cannot be limited to identifying its existence or cataloguing its forms; it must also examine the depth and breadth of its impact on tourists and destinations. In the Arab context, cybercrime has revealed structural vulnerabilities that extend beyond individual incidents, reflecting broader deficiencies in digital governance, legal preparedness, and institutional coordination. These vulnerabilities affect not only tourists' material interests but also their perceptions of safety, trust in tourism institutions, and willingness to engage with digital tourism services [17].

Cybercrime in tourism operates within a complex ecosystem characterized by data intensity, interdependence among multiple actors, and cross-border digital transactions. As a result, the consequences of cyber incidents tend to cascade across the tourism value chain, affecting tourists, service providers, and destination reputation simultaneously. This section focuses on examining cybercrimes from an impact-oriented perspective, emphasizing how different forms of digital crime affect the Arab tourist at both individual and collective levels.

This section is structured into three main parts. The first examines the impact of cybercrime on the Arab tourist, the second analyzes the classification of tourism-related cybercrimes, and the third explores their broader effects on tourist confidence and destination image.

A) The Impact of Cybercrime on the Arab Tourist:

The impact of cybercrime on the Arab tourist extends beyond immediate financial loss. Cyber incidents generate a persistent sense of insecurity, eroding trust in digital tourism services and influencing tourists' behavior. Many tourists become reluctant to use online booking platforms, electronic payment systems, or mobile travel applications, preferring traditional and less efficient alternatives. This phenomenon contributes to what has been described as "digital travel anxiety," which affects the quality of the tourism experience and reduces the benefits of digital innovation [18.]

At a broader level, cybercrime affects destination image and competitiveness. Tourist destinations perceived as digitally unsafe may suffer reputational damage, leading to reduced tourist flows and diminished investment in the tourism sector. In an increasingly competitive global tourism market, digital security has become a decisive factor in destination choice, alongside traditional considerations such as cultural attractions and physical safety.

In the Arab world, the absence of clear reporting mechanisms and effective legal remedies further aggravates the impact of cybercrime on tourists. Victims often face difficulties in reporting digital offenses, identifying responsible parties, or obtaining compensation, particularly in cross-border cases involving foreign platforms. This lack of institutional support reinforces feelings of vulnerability and undermines confidence in tourism governance structures.

The examination of cybercrime in the tourism sector demonstrates that digital threats have become a structural component of tourism insecurity rather than an exceptional phenomenon. The increasing reliance on digital platforms and data-driven services has exposed tourists to new forms of risk that transcend territorial boundaries and challenge traditional legal responses. In the Arab context, these risks are amplified by regulatory fragmentation and limited sector-specific protection mechanisms [19].

Cybercrime affects tourists at multiple levels, from direct financial loss to long-term erosion of trust in digital tourism services. The absence of effective reporting mechanisms and legal remedies further aggravates tourists' vulnerability and reinforces perceptions of insecurity. This analysis confirms that addressing cybercrime requires an integrated approach that combines legal reform, institutional coordination, and preventive strategies, thereby linking tourism security directly to broader issues of digital governance and consumer protection 20.

The impact of cybercrime on the tourist must be examined through the lens of legal protection afforded to the tourist as a digital consumer. In digital tourism transactions, tourists are not merely service users but parties to electronic contracts governed by consumer protection principles. Cyber incidents such as fraudulent bookings or unauthorized transactions directly infringe contractual rights and undermine the principle of informed consent, which constitutes a cornerstone of consumer law21.

Moreover, data breaches affecting tourists engage the legal responsibility of tourism service providers with regard to data security obligations. Contemporary legal frameworks increasingly recognize that failure to implement adequate technical and organizational measures may give rise to civil liability, administrative sanctions, or both. However, in the Arab context, the absence of clear procedural mechanisms often limits tourists' access to remedies, particularly in cross-border digital transactions involving foreign platforms 22.

This legal gap reinforces the vulnerability of Arab tourists and highlights the need to strengthen legal safeguards ensuring effective redress, compensation, and accountability in cases of tourism-related cybercrime.

B) Classification of Tourism Cybercrimes and Analysis of Their Impact on the Tourist:

Tourism-related cybercrimes can be classified according to the nature of the targeted interest and the stage of the travel process in which they occur. A first category includes crimes targeting tourists' financial interests, such as online booking fraud, fake travel agencies, and unauthorized electronic transactions. These crimes exploit tourists' reliance on digital platforms and often result in immediate financial loss, as well as subsequent difficulties in recovering funds or identifying perpetrators[23].

A second category concerns crimes targeting tourists' personal data and privacy. The tourism sector processes highly sensitive information, including identification documents, payment details, travel itineraries, and accommodation records. Unauthorized access to hotel databases, airline reservation systems, or online travel platforms can lead to large-scale data breaches. For tourists, the consequences extend beyond the travel context, exposing them to identity theft, financial fraud, and long-term misuse of their personal information [24].

It should be emphasized that, as previously discussed, several Arab countries have adopted legal frameworks addressing cybercrime that are applicable to tourism-related digital activities. In North Africa, Algeria's Law [25]No. 09-04 criminalizes unauthorized access to information systems and data interference, which directly applies to attacks on tourism platforms, while Tunisia's Law[26] No. 2004-5 on the security of information systems penalizes illegal access to information systems and data-related offenses. In the Middle East, Egypt's Law[27] No. 175 of 2018, particularly Articles 18, 23, and 24, addresses unlawful access, data breaches, and electronic fraud, whereas Saudi Arabia's Anti-Cyber Crime Law (Royal Decree No. M/17 of 2007)[28], notably Article 3, criminalizes financial fraud and unauthorized access to information systems. These examples demonstrate that legal protection exists across different Arab regions, although its application to tourism remains indirect.

A third category involves crimes targeting the operational integrity of tourism institutions, such as ransomware attacks, system disruptions, and denial-of-service attacks. Although tourists may not be the direct targets of these crimes, they are indirectly affected through service interruptions, flight cancellations, booking failures, and loss of access to travel-related information. Such incidents demonstrate the strong interdependence between institutional cybersecurity and tourist protection, highlighting that the security of tourism infrastructure is inseparable from the security of tourists themselves [29].

From the perspective of the Arab tourist, these different categories of cybercrime share a common effect: the creation of a persistent sense of uncertainty regarding the reliability of digital tourism services. The absence of clear information about security standards and the lack of transparency in handling cyber incidents exacerbate this uncertainty, reinforcing tourists' perceptions of vulnerability in digital environments.

C) The Impact of Digital Crimes on the Confidence of the Arab Tourist and the Image of Tourist Destinations:

Beyond individual harm, cybercrimes exert a broader impact on tourist confidence and destination image. Trust constitutes a central element of the tourism experience, particularly in digital contexts where tourists must rely on remote services and intangible assurances. Cyber incidents undermine this trust by revealing weaknesses in data protection, risk management, and institutional accountability [30].

In the Arab context, the erosion of digital trust is particularly significant due to the cultural importance attached to privacy, personal reputation, and financial security. Even isolated cyber incidents may generate widespread concern among tourists, leading to generalized perceptions of risk that affect destination choice. As a result, destinations associated with recurring digital security failures may be perceived as unsafe, regardless of their physical security conditions or tourism attractions [31].

The impact of cybercrime on destination image also has economic implications. Reduced trust in digital tourism services can lead to decreased online bookings, lower tourist flows, and diminished investment in tourism infrastructure. In an increasingly competitive global tourism market, destinations that fail to ensure adequate digital protection risk losing their comparative advantage. Digital security has thus become a strategic component of destination competitiveness, alongside traditional factors such as accessibility and service quality [32].

At the behavioral level, the accumulation of cyber incidents contributes to changes in tourist practices. Many tourists adopt defensive strategies, such as limiting online transactions, avoiding unfamiliar platforms, or relying on cash payments instead of electronic methods. While these behaviors may reduce individual risk, they also undermine the efficiency and innovation potential of digital tourism systems, ultimately affecting the overall quality of the tourism experience.

The impact-oriented analysis of tourism-related cybercrimes reveals that their consequences extend far beyond individual victimization. Cyber incidents undermine tourist confidence, alter travel behavior, and affect destination image and competitiveness. In the Arab world, where tourism development increasingly depends on digital channels, the erosion of digital trust constitutes a significant obstacle to sustainable tourism growth [33].

Moreover, the cumulative effect of cyber incidents contributes to the emergence of defensive tourist behaviors that limit the benefits of digital innovation. These dynamics demonstrate that cybercrime represents not only a criminal or technical issue, but also a strategic challenge with economic, social, and reputational dimensions. Addressing these impacts requires rethinking tourism security as an integral component of destination governance and long-term development strategies [34].

These challenges are further compounded at the international level by the absence of a comprehensive and binding legal framework specifically addressing cybercrime in the tourism sector. While certain international instruments contribute indirectly to tourist protection, they do not provide a sector-specific response to digital risks affecting tourism activities. For instance, the International Code for the Protection of Tourists establishes general principles related to tourist protection and assistance, but does not explicitly regulate cyber threats. Similarly, the Budapest Convention on Cybercrime provides a global legal framework for combating cybercrime, yet it remains general in scope and not tailored to the specificities of tourism-related digital risks. This normative gap at the intersection of tourism law and cybersecurity contributes to the persistence of vulnerabilities identified in this section, reinforcing the need for integrated legal and governance responses.

In light of these limitations, the need to move beyond fragmented and reactive approaches becomes increasingly evident. This calls for the development of an integrated model of smart tourism security capable of addressing digital risks through coherent legal, institutional, and preventive frameworks.

Section IV: Toward an Arab Model of Smart Tourism Security.

The necessity of developing an Arab model of smart tourism security becomes evident when considering the cumulative weaknesses identified in traditional tourism security frameworks and the growing exposure of tourists to digital risks. The persistence of reactive security approaches, combined with fragmented legal regulation and limited institutional coordination, has created a structural gap between the realities of digital tourism and the mechanisms available to protect tourists. In an environment where tourism activities increasingly depend on digital platforms and data-driven systems, security can no longer be addressed through isolated measures or sectoral interventions [35].

Smart tourism security must therefore be understood as a governance-based model that integrates legal norms, institutional arrangements, technological safeguards, and preventive strategies within a unified framework. This model seeks not only to respond to incidents after they occur, but also to anticipate risks, reduce vulnerabilities, and strengthen resilience across the tourism ecosystem. In the Arab context, adopting such a model represents a strategic choice linked to destination competitiveness, tourist confidence, and sustainable tourism development.

This section is organized into three main components. It first examines the legal foundations of smart tourism security, then analyzes institutional governance and preventive mechanisms, and finally presents a comparative perspective.

A) Legal Foundations of Smart Tourism Security:

The legal dimension constitutes the cornerstone of any effective smart tourism security model. In many Arab countries, tourism legislation remains primarily administrative in nature, focusing on licensing, classification, and supervision of tourism establishments. While these regulatory functions are essential, they do not address the complex digital risks associated with modern tourism activities. As a result, tourism security lacks a clear legal identity and remains dependent on general criminal law or fragmented cybersecurity regulations.

It should be emphasized that, as previously discussed, several Arab countries have adopted legal frameworks addressing cybercrime and data protection, which are directly applicable to tourism-related digital activities. In Algeria, Law No. 09-04, particularly provisions criminalizing unauthorized access to information systems and data interference, provides a legal basis for addressing attacks on tourism platforms. Similarly, Egypt's Law No. 175 of 2018, notably Articles 18, 23, and 24, establishes sanctions for unlawful access, data breaches, and electronic fraud, which are frequently encountered in online booking and payment systems.

In Saudi Arabia, Article 3 of the Anti-Cyber Crime Law criminalizes financial fraud and illegal access to information systems, offering protection against fraudulent tourism transactions. Jordan's

Cybercrime Law No. 27 of 2015 and Qatar's Law No. 14 of 2014 also include provisions addressing unauthorized access and misuse of digital data, thereby extending legal protection to tourists as users of digital services.

These legal provisions demonstrate that cybercrime affecting tourism activities is already covered under existing legislative frameworks. However, their application remains indirect, as they are not specifically designed to address the particular risks associated with digital tourism environments. This confirms that the issue lies not in the absence of legal regulation, but in its fragmented and non-sector-specific nature.

From a legal perspective, these situations also raise issues of consumer protection and civil liability. Tourists, as digital consumers, engage in electronic transactions that are subject to principles of transparency, security, and informed consent. Cyber incidents such as fraudulent bookings or data breaches may therefore constitute not only criminal offenses, but also violations of contractual obligations and consumer protection standards, potentially giving rise to civil liability for service providers who fail to implement adequate security measures.

In parallel, institutional mechanisms such as specialized tourist police units contribute to enhancing tourist protection, including in cases involving fraud and digital exploitation. Nevertheless, these mechanisms remain complementary and do not compensate for the absence of sector-specific legal provisions.

Therefore, the main challenge lies not in the absence of legal frameworks, but in their fragmentation and the lack of integration between tourism legislation and cybersecurity laws, which limits their effectiveness in addressing the specific risks of digital tourism.

A smart tourism security framework requires explicit legal recognition of tourism security as a multidimensional concept encompassing physical safety, digital protection, data security, and consumer rights. Tourism laws should therefore be revised to incorporate provisions on cybersecurity obligations, personal data protection, and risk management specific to tourism activities. Such provisions would establish clear standards for tourism institutions and reduce legal uncertainty regarding their responsibilities toward tourists.

Data protection represents a particularly critical legal pillar. Tourism institutions process large volumes of sensitive personal data, often across borders and through third-party platforms. Without binding legal obligations, data protection practices remain uneven and largely dependent on voluntary compliance. Integrating data protection requirements into tourism legislation strengthens accountability and enhances tourists' trust in digital services, especially in regions where awareness of digital rights remains limited [36].

Legal clarity regarding liability is another essential component. The digital tourism ecosystem involves multiple actors whose roles and responsibilities often overlap. In cases of cyber incidents, tourists frequently face difficulties identifying the responsible party or obtaining compensation. A smart tourism security framework must therefore establish clear rules allocating civil and administrative liability among tourism service providers, digital platforms, and intermediaries. Such clarity not only protects tourists but also incentivizes institutions to invest in preventive cybersecurity measures [37].

Furthermore, legal frameworks should incorporate preventive regulatory tools, such as mandatory cybersecurity audits, certification schemes for secure tourism platforms, and compliance requirements aligned with international standards. These tools contribute to shifting tourism security from a reactive logic toward an anticipatory approach based on risk assessment and continuous improvement. By embedding prevention into legal norms, tourism security becomes a proactive governance mechanism rather than an emergency response function [38].

At the international level, the legal foundations of smart tourism security are increasingly shaped by normative instruments addressing tourist protection and digital rights. The **International Code for the Protection of Tourists (ICPT)** adopted by the UNWTO in 2022 constitutes a significant reference in this regard. Although the Code is not legally binding, it establishes clear principles concerning the protection of tourists, access to assistance, and the responsibility of States and service providers in crisis situations, including those involving digital risks [39].

In parallel, international data protection and digital services regulations, particularly the **General Data Protection Regulation (GDPR)** and the **Digital Services Act (DSA)** of the European Union, have set de facto global standards. These instruments impose strict obligations regarding data processing, platform accountability, and risk management, directly affecting tourism operators worldwide, including those operating in or targeting Arab markets through global platforms [40].

Despite the existence of these international and comparative standards, Arab tourism legislation remains largely silent on digital tourism security. Tourism laws in most Arab countries continue to focus on administrative regulation, licensing, and service quality, without explicitly addressing cybersecurity obligations, data protection duties, or digital risk management in the tourism sector. This normative gap results in a fragmented legal landscape in which cybersecurity and data protection laws, where they exist, operate in isolation from tourism legislation, thereby weakening their effectiveness in protecting tourists[41]. The absence of explicit legal recognition of digital tourism security underscores the urgent need to integrate international standards into Arab tourism law as a foundational element of any smart tourism security model.

It is noteworthy that, although the Arab Tourism Strategy emphasizes the importance of tourism security as a key factor for enhancing competitiveness and improving the image of Arab destinations, it does not explicitly address cybercrime-related threats. This reflects the persistence of a traditional approach to tourism security, primarily focused on physical dimensions, while the digital transformation of tourism has generated new risks that transcend territorial boundaries. Consequently, cybercrime emerges as a contemporary challenge that exacerbates the vulnerabilities identified in the strategy, particularly in relation to tourist trust and destination image. This calls for a reconceptualization of tourism security to incorporate digital dimensions within an integrated governance framework.

B) Institutional Governance and Preventive Mechanisms:

Legal reform alone is insufficient without effective institutional governance capable of implementing and enforcing security standards. In the Arab context, tourism security governance is often characterized by institutional dispersion, with responsibilities shared among tourism authorities, internal security agencies, telecommunications regulators, and cybersecurity bodies. This fragmentation undermines coordination, delays response to incidents, and weakens accountability [42].

A smart tourism security model requires the establishment of clear institutional coordination mechanisms. This includes defining the roles of each authority, creating formal channels for information sharing, and ensuring joint response procedures in cases of cyber incidents affecting tourists. Institutional coherence is essential to transform legal norms into effective protection mechanisms and to avoid gaps in enforcement.

The creation of specialized tourism cybersecurity units within national tourism authorities or tourism ministries constitutes a key institutional innovation. These units would serve as focal points for monitoring digital threats, coordinating responses with cybersecurity agencies, and providing guidance to tourism institutions and tourists alike. By centralizing expertise, such units enhance institutional capacity and improve crisis management in the tourism sector [43].

Preventive mechanisms are a central feature of smart tourism security. Beyond technological solutions, prevention involves awareness-raising, training, and behavioral adaptation. Tourists must

be informed about digital risks, safe booking practices, and secure payment methods, while tourism professionals require training on data protection, incident reporting, and cybersecurity best practices. Preventive education reduces vulnerability and complements legal and technical measures.

Early-warning systems and information-sharing platforms also play a crucial role in prevention. By detecting emerging threats and disseminating timely alerts, authorities and institutions can respond proactively and limit the spread of cyber incidents. At the regional and universal levels, cooperation mechanisms enable the exchange of intelligence and best practices, addressing the transnational nature of tourism-related cybercrime [44].

Ultimately, institutional governance and preventive mechanisms transform tourism security into a dynamic and adaptive system. Rather than relying on isolated interventions, smart tourism security integrates law, institutions, and prevention within a coherent governance framework. For Arab countries, adopting this approach offers a pathway to enhancing tourist protection, restoring digital trust, and strengthening the resilience and competitiveness of their tourism sectors in an increasingly interconnected world.

C) Comparative Perspective on Smart Tourism Security Models:

A comparative examination of international experiences highlights the growing centrality of smart tourism security in contemporary tourism governance. In several regions, particularly within the European Union, tourism security has progressively evolved toward integrated frameworks that combine data protection, cybersecurity regulation, and consumer rights. Legal instruments such as the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA) establish binding obligations for service providers and enhance accountability in digital environments, thereby strengthening tourists' trust in online tourism services [45].

At the institutional level, many destinations have adopted coordinated governance models that link tourism authorities with cybersecurity agencies and consumer protection bodies. These arrangements facilitate information sharing, incident response, and preventive oversight, reducing the fragmentation that characterizes traditional security approaches. International organizations, notably the UNWTO and the OECD, emphasize the importance of aligning tourism security policies with broader digital governance strategies, recognizing cybersecurity as a core component of tourism quality and competitiveness [46].

In comparison, Arab tourism security frameworks remain largely focused on physical protection and administrative regulation, with limited integration of digital security considerations. While some countries have adopted cybersecurity laws or national digital strategies, these instruments are often disconnected from tourism policy and lack sector-specific implementation mechanisms. This gap highlights the need for an adapted Arab model that draws on international standards while addressing regional legal, institutional, and cultural specificities.

A closer analysis reveals significant differences between European and Arab approaches to tourism security in the digital context. Within the European Union, a comprehensive and integrated legal framework governs digital risks affecting tourists. Instruments such as the **General Data Protection Regulation (GDPR),** the **Digital Services Act (DSA),** and the **Budapest Convention on Cybercrime** establish clear obligations regarding data protection, platform accountability, and international cooperation. These frameworks provide a high level of legal certainty and ensure effective protection for tourists engaging in digital transactions.

In contrast, Arab legal systems remain characterized by fragmentation and limited sector-specific integration. While several Arab countries have adopted cybercrime laws and data protection regulations, these frameworks often operate independently from tourism legislation and lack coordinated implementation mechanisms. This results in legal uncertainty, difficulties in determining liability, and limited access to remedies for tourists, particularly in cross-border digital contexts

The comparative perspective demonstrates that smart tourism security is not merely a technical option, but a strategic requirement for destinations seeking to enhance resilience and competitiveness in a globalized tourism market. For Arab countries, integrating lessons from international experiences into a coherent and context-sensitive framework represents a critical step toward strengthening tourist protection and rebuilding digital trust[47].

A comparative analysis reveals that, unlike European legal systems, most Arab tourism laws do not explicitly address digital security or cyber risks affecting tourists. Tourism legislation in the Arab world continues to focus primarily on administrative regulation, licensing, and service quality, without incorporating binding obligations related to data protection, cybersecurity, or digital risk management[48].

This normative silence contrasts sharply with international and comparative trends, where tourism security is increasingly embedded within broader digital governance frameworks. The lack of explicit legal provisions addressing digital tourism security results in fragmented protection and weak enforcement, leaving tourists exposed to cyber risks without clear legal guarantees.

Addressing these normative gaps requires not merely the adoption of cybersecurity laws, but their effective integration into tourism legislation through explicit provisions recognizing digital security as an essential component of tourist protection.

The analysis of legal and institutional dimensions of smart tourism security confirms that fragmented and reactive approaches are inadequate to protect tourists in a digitalized tourism environment. Effective tourism security requires coherent legal frameworks, clear allocation of responsibilities, and robust institutional coordination mechanisms. Without these elements, preventive strategies and technological solutions remain limited in their effectiveness.

The development of an Arab model of smart tourism security must therefore be grounded in governance principles that integrate law, institutions, and prevention. Such a model enhances not only tourist protection but also destination resilience and competitiveness. By embedding security within tourism governance, Arab countries can respond more effectively to digital risks while aligning their tourism sectors with international standards and best practices.

Conclusion

This study demonstrates that the evolution of tourism security in the Arab world is marked by a structural imbalance between the rapid digitalization of tourism activities and the persistence of fragmented legal and institutional frameworks. This imbalance has transformed tourism security from a traditional protection function into a complex governance challenge.

The findings confirm that cybercrime constitutes a systemic risk affecting not only individual tourists but also the functioning of tourism systems and the competitiveness of destinations. Its impact extends beyond immediate financial harm to include legal uncertainty, weakened trust in digital services, and reputational risks at both institutional and destination levels.

From a legal perspective, the study establishes that the main limitation does not lie in the absence of regulatory frameworks, but in their lack of integration and sector-specific adaptation. The disconnection between tourism legislation, cybercrime laws, and data protection regimes generates uncertainty in the allocation of liability and limits the effectiveness of legal remedies, particularly in cross-border digital contexts.

At the institutional level, the dispersion of responsibilities and the absence of coordinated governance mechanisms significantly reduce the capacity to address cyber risks in a coherent and preventive manner. This confirms that tourism security cannot be effectively ensured through isolated interventions, but requires an integrated governance approach.

Furthermore, the analysis highlights that cyber risks directly influence tourist behavior and destination image, making digital trust a decisive factor in tourism demand and competitiveness. In this context, cybersecurity emerges as a strategic component of tourism governance rather than a purely technical issue.

On this basis, the study concludes that strengthening tourism security in the Arab world requires a shift from reactive and fragmented approaches toward an integrated model of smart tourism security. Such a model must be based on legal coherence, institutional coordination, and preventive governance, and should recognize digital security as a core dimension of tourist protection and sustainable tourism development.

Recommendations

In light of these findings, the following recommendations are proposed:

– Modernize tourism legislation by explicitly incorporating cybersecurity and data protection obligations within sector-specific regulations.
– Ensure legal integration between tourism law, cybercrime frameworks, and data protection regimes in order to clarify liability and enhance legal certainty.
– Establish coordinated institutional mechanisms, including specialized tourism cybersecurity units, to improve risk management and incident response.
– Develop preventive security strategies based on risk assessment, early-warning systems, and continuous monitoring of digital threats.
– Promote digital awareness among tourists and tourism professionals to strengthen preventive protection.
– Implement accessible reporting and redress mechanisms to improve accountability and trust.
– Strengthen regional and universal cooperation to address the transnational nature of cybercrime.
– Integrate tourism security into broader digital transformation and sustainable development strategies.

Citations:

[1] UN World Tourism Organization (UNWTO), *Crisis Management Guidelines for the Tourism Sector*, Madrid; 2019.
[2] UN World Tourism Organization (UNWTO), *Global Guidelines to Restart Tourism*, Madrid; 2020.
[3] UN World Tourism Organization (UNWTO), *Recommendations for the Transition to a Green and Safe Tourism*, Madrid; 2021.
[4] UN World Tourism Organization (UNWTO), *Digital Futures Programme Reports*, Madrid; 2022–2023.
[5] UN World Tourism Organization (UNWTO); World Health Organization (WHO), *Tourism and COVID-19: Travel and Health Guidelines*, Geneva; 2020.
[6] UN World Tourism Organization (UNWTO), *International Code for the Protection of Tourists (ICPT)*, Madrid; 2022.
[7] Hall, C. M.; Timothy, D., *Tourism and Security: Contemporary Issues: Global Perspectives on Risk and Security*, Routledge, United Kingdom, 2020, pp. 45–52.
Tarlow, P., *Tourism Security: Strategies for Effectively Managing Travel Risk and Safety*, Elsevier, 2021, pp. 33–41.
[8] UN World Tourism Organization (UNWTO), *International Code for the Protection of Tourists (ICPT)*, op.cit.
[9] Organisation for Economic Co-operation and Development (OECD), *Tourism Trends and Policies 2022*, Paris; 2022.
[10] Organisation for Economic Co-operation and Development (OECD), *Tourism Trends and Policies 2023*, Paris; 2023.

[11] INTERPOL, *Cybercrime: Assessment Report*, Lyon; 2021.
[12] INTERPOL, *Global Crime Trend Report*, Lyon; 2022.
[13] INTERPOL, *Cybercrime Related to the COVID-19 Pandemic*, Lyon; 2020–2021.
[14] INTERPOL, *Cybercrime: op.cit.*
INTERPOL, *Global Crime Trend Report*, op.cit.
[15] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape (ETL 2022)*, Athens; 2022.
[16] European Union Agency for Cybersecurity (ENISA), op.cit.
[17] European Commission, *Regulation (EU) 2016/679 – op.cit.*
[18] European Union Agency for Cybersecurity (ENISA), op.cit.
[19] INTERPOL, *Cybercrime: Assessment Report*, Lyon; 2021.
INTERPOL, *Global Crime Trend Report*, op.cit.
[20] European Union Agency for Cybersecurity (ENISA), op.cit.
European Union Agency for Cybersecurity (ENISA), *Cybersecurity for SMEs: Challenges and Recommendations*, Athens; 2021.
[21] European Commission, *Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR)*, Official Journal of the European Union; 2016.
[22] European Commission, *Regulation (EU) 2022/2065 – Digital Services Act (DSA)*, Official Journal of the European Union; 2022.
GCC Cybersecurity Centre, *Cyber Risks in Gulf Tourism*, GCC; 2022.
[23] European Commission, *Regulation (EU) 2022/2065 – op.cit.*
[24] World Economic Forum, *Global Cybersecurity Outlook*, Geneva; 2022.
[25] Law No. 09-04 of 14 Sha'ban 1430 corresponding to August 5, 2009, on Specific Rules on the Prevention and Fight Against Information Technologies and Communication's Crimes, Algeria Available at: https://www.wipo.int/wipolex/en/legislation/details/14778
[26] Tunisia Law No. 2004-5 on the security of information systems.: https://legislation-securite.tn/latest-laws/loi-n-2004-5-du-3-fevrier-2004-relative-a-la-securite-informatique/
[27] Egyptian law No. 175 of 2018 On Anti-Cyber and Information Technology Crimes https://eg.andersen.com/translation-law-175-2018/
https://cybercrime-fr.org/wp-content/uploads/2020/04/Egyptian-cybercrime-law-.pdf
[28] Saudi Arabia's Anti-Cyber Crime Law (Royal Decree No. M/17 of 2007 https://www.wipo.int/wipolex/en/text/498373
https://www.chathamhouse.org/2018/07/cybercrime-legislation-gcc-countries/cybercrime-legislation-comparing-global-and-gcc
[29] Hall, C. M.; Timothy, D, op.cit. pp. 45–52
[30] Tarlow, P., op.cit. pp. 33–41
[31] Paraskevas, A.; Quek, M., "When Cybersecurity Threats Hit the Tourism Sector", *Journal of Travel Research*, Vol. 59, No. 6, 2020, pp. 1001–1015.
[32] Celdrán-Bernabéu, M. A.; Mazón, J.-N.; Giner-Sánchez, D.; Morales-García, J.; Peñarrubia-Zaragoza, M. P. (2025), *Smart Tourism Destinations as Open Data Providers: Barriers and Opportunities, Tourism Management Perspectives*. Available at: https://www.sciencedirect.com/science/article/pii/S2212571X25000770 (consulted on 20/03/2025)
[33] Tan, Y.; Jiang, G.; Merajuddin, S. S.; Zhao, F. (2025), *Analyzing the Impact of Digital Technology on Consumers' Travel Intentions* Journal of Innovation & Knowledge. Available at: https://www.sciencedirect.com/science/article/pii/S2444569X25000356 (consulted on 21/03/2025).
Florido-Benítez, L. (2025), The Role of Cybersecurity as a Preventive Measure in Digital Tourism and Travel: A Systematic Literature Review, Discover Computing. Available at: https://link.springer.com/article/10.1007/s10791-025-09523-3 (consulted on 21/03/2025).
[34] World Economic Forum, op.cit.
[35] Tan, Y.; Jiang, G.; Merajuddin, S. S.; Zhao, F. (2025), J., op.cit.

[36] Bada, Maria; Sasse, Angela M.; Nurse, Jason R.C., "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?", Global Cyber Security Capacity Centre, University of Oxford. . Available at: https://www.cs.ox.ac.uk/files/7194/csss2015_bada_et_al.pdf
Dupont, Benoît; Whelan, Chad (2021), "Enhancing Relationships between Criminology and Cybersecurity", Université de Montréal. Available at: https://benoitdupont.openum.ca/files/sites/31/2021/04/Dupont-Whelan-2021-Enhancing-relationships.pdf (consulted on 21/03/2025).
[37] GCC Cybersecurity Centre, *Cyber Risks in Gulf Tourism*, GCC; 2022.
[38] Saudi Tourism Authority, *Digital Tourism Safety Report*, Riyadh, 2023, pp.7-11.
[39] UN World Tourism Organization (UNWTO), *International Code for the Protection of Tourists (ICPT)*, op.cit.
[40] European Commission, *Regulation (EU) 2016/679 – op.cit.*
European Commission, *Regulation (EU) 2022/2065 – op.cit.*
[41] Arab Tourism Organization, *Tourism Development and Security in the Arab World*, Cairo; 2022.
[42] UAE Cybersecurity Council, *Cyber Safety Framework for Tourism*, Abu Dhabi; 2022. Available at*: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security* (consulted on 21/03/2025).
[43] Centre for Mediterranean Tourism Studies, *Tourism Digital Security in North Africa*, 2021.
[44] Arab Tourism Organization, op.cit.
[45] European Commission, *Regulation (EU) 2016/679 – op.cit.*
European Commission, *Regulation (EU) 2022/2065 – op.cit.*
[46] Organisation for Economic Co-operation and Development (OECD), *Tourism Trends* and *Policies 2022*, op.cit.
Organisation for Economic Co-operation and Development (OECD), *Tourism Trends and Policies 2023*, op.cit.
[47] World Economic Forum, Global Cybersecurity Outlook, op.cit.
[48] Celdrán-Bernabéu, M. A.; Mazón, J.-N.; Giner-Sánchez, D.; Morales-García, J.; Peñarrubia-Zaragoza, M. P. (2025). op.cit.

Bibliography:

A- Books:

- Hall, C. M.; Timothy, D. J., *Tourism and Security: Contemporary Issues*, 2nd edition, Routledge, United Kingdom, 2020.
- Tarlow, P., *Tourism Security: Strategies for Effectively Managing Travel Risk and Safety*, Elsevier, United Kingdom, 2014.

B- Journal Articles:

- Paraskevas, A.; Quek, M., "When Cybersecurity Threats Hit the Tourism Sector", *Journal of Travel Research*, Vol. 59, No. 6, 2020.
- Celdrán-Bernabéu, M. A.; Mazón, J.-N.; Giner-Sánchez, D.; Morales-García, J.; Peñarrubia-Zaragoza, M. P. (2025), "Smart Tourism Destinations as Open Data Providers: Barriers and Opportunities", Tourism Management Perspectives.
- Tan, Y.; Jiang, G.; Merajuddin, S. S.; Zhao, F. (2025), Analyzing the Impact of Digital Technology on Consumers, Travel Intentions, Journal of Innovation & Knowledge.
- Florido-Benítez, L. (2025), *The Role of Cybersecurity as a Preventive Measure in Digital Tourism and Travel: A Systematic Literature Review, Discover Computing.*
- Bada, Maria; Sasse, Angela M.; Nurse, Jason R.C., "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?", Global Cyber Security Capacity Centre, University of Oxford.

- Dupont, Benoît; Whelan, Chad (2021), "Enhancing Relationships between Criminology and Cybersecurity", Université de Montréal.

C- Websites:

- UN World Tourism Organization (UNWTO), International Code for the Protection of Tourists (ICPT), Madrid, 2022. Available at: https://www.e-unwto.org/doi/10.18111/9789284423484 (consulted on 7/02/2025).
- European Union, *Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR)*, Official Journal of the European Union, 2016. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (consulted on 7/02/2025).
- European Union, *Regulation (EU) 2022/2065 – Digital Services Act (DSA)*, Official Journal of the European Union, 2022. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (consulted on 08/02/2025).
- • OECD, *Digital Security Risk Management*, OECD Publishing, Paris. Available at: https://www.oecd.org/digital/digital-security-risk-management.htm (consulted on 09/02/2025).
- • INTERPOL, *Cybercrime: Assessment Report*, Lyon, 2021. Available at: https://www.interpol.int/en/Crimes/Cybercrime (consulted on 09/02/2025).
- • European Union Agency for Cybersecurity (ENISA), *Cybersecurity and Tourism*, ENISA Publications. Available at: https://www.enisa.europa.eu/publications (consulted on 10/02/2025).
- Arab Tourism Organization, Tourism Development and Security in the Arab World, Cairo, 2022. Available at: https://www.arabtourismorg.org.sa/ (consulted on 20/03/2025).
- UAE Cybersecurity Council, Cyber Safety Framework for Tourism, Abu Dhabi, 2022. Available at: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security (consulted on 20/03/2022).