

"الأمن السيبراني وحماية السائح في السياحة الرقمية:

إدارة مستدامة للبيانات والتدفقات"

Cybersecurity and Tourist Protection in Digital Tourism: "

"Sustainable Management of Data and Flows

أ. د/ رحمون صافية، كلية الحقوق والعلوم السياسية، – جامعة تيبازة – الجزائر

<https://orcid.org/0009-0000-2107-4226> / rahmoune.safia@cu-tipaza.dz

تاريخ الاستلام: 2026/01/23 تاريخ القبول: 2026/05/25 تاريخ النشر: 2026/06/20

الملخص

تتناول هذه الدراسة، موضوع السياحة الرقمية في ظل تصاعد المخاطر السيبرانية المرتبطة باستعمال المنصات الذكية في تقديم الخدمات السياحية. وتكمن أهمية الموضوع في كونه يمس حماية السائح الرقمي وضمان استدامة النشاط السياحي في البيئة الرقمية. وتتمحور إشكالية الدراسة حول مدى كفاية آليات الأمن السيبراني في حماية البيانات الشخصية والمالية للسائح. وقد خلصت الدراسة إلى أن تعزيز التشفير، والتحقق متعدد العوامل، واعتماد مقاربة وقائية قانونية، يساهم في تقليص المخاطر السيبرانية وترسيخ سياحة رقمية آمنة ومستدامة.

الكلمات المفتاحية: الأمن السيبراني، حماية السائح، السياحة الرقمية، إدارة البيانات، استدامة الوجهات.

Abstract

This paper addresses digital tourism in light of the growing cyber risks associated with the use of smart platforms in the provision of tourism services. The importance of the topic lies in its relevance to protecting the digital tourist and ensuring the sustainability of tourism activities in the digital environment. The study examines the extent to which cybersecurity mechanisms are sufficient to safeguard tourists' personal and financial data. The findings reveal that strengthening encryption, implementing multi-factor authentication, and adopting a preventive legal approach contribute to reducing cyber risks and fostering secure and sustainable digital tourism.

key words: Cybersecurity, tourist protection, digital tourism, data management, destination sustainability.

مقدمة:

أفرز التحول الرقمي المتسارع الذي تشهده الدول العربية أنماطاً جديدة في النشاط السياحي، حيث أصبح الاعتماد على المنصات الرقمية في الحجز والدفع وتبادل المعلومات عنصراً جوهرياً في التجربة السياحية المعاصرة. ورغم ما أتاحه هذا التحول من فرص لتطوير الخدمات السياحية وتعزيز جاذبية الوجهات، فإنه في المقابل أفرز مخاطر سيبرانية متزايدة، لاسيما تلك المرتبطة بالاعتداء على البيانات الشخصية والمالية للسائح، بما يهدد الثقة الرقمية واستدامة النشاط السياحي.

وتكتسي دراسة الأمن السيبراني في المجال السياحي أهمية خاصة، لكونها تمس حماية السائح باعتباره طرفاً ضعيفاً في البيئة الرقمية، وتسهم في دعم تنافسية الوجهات السياحية وتحقيق التنمية السياحية المستدامة. وانطلاقاً من ذلك، تطرح الدراسة الإشكالية الآتية: إلى أي مدى يمكن لآليات الأمن السيبراني المعتمدة في القطاع السياحي العربي توفير حماية فعّالة للسائح في ظل تصاعد الجرائم الإلكترونية؟

وتهدف هذه الدراسة إلى تحليل أبرز التهديدات السيبرانية التي تستهدف السائح في السياحة الرقمية العربية، وبيان دور الاستراتيجيات الحديثة للأمن السيبراني في حماية البيانات وتعزيز الثقة الرقمية، فضلاً عن إبراز العلاقة بين الأمن الرقمي واستدامة الوجهات السياحية. ولتحقيق هذه الأهداف، تم اعتماد المنهج التحليلي بالأساس، مدعماً بالمنهج الاستقرائي من خلال دراسة المفاهيم القانونية والوقوف على التطبيقات العملية ذات

الصلة، مع تقسيم الدراسة وفق خطة منهجية توازن بين التأصيل النظري والتحليل التطبيقي.

المحور الأول: التأصيل المفاهيمي للأمن السيبراني في البيئة السياحية الرقمية

لم يعد الأمن السيبراني في السياحة الرقمية مجرد منظومة تقنية لحماية الأنظمة المعلوماتية، بل أضى إطاراً وظيفياً متكاملًا يهدف إلى تأمين الفضاء السياحي الرقمي وحماية السائح بوصفه طرفاً ضعيفاً في العلاقات الرقمية. ويقتضي التأصيل النظري لهذا المجال تجاوز المقاربات التقنية الصرفة، نحو فهم الأمن السيبراني كآلية وقائية توازن بين تسهيل الخدمات السياحية الرقمية وضمان سلامة البيانات الشخصية والمالية. ومن ثم، يشكل هذا التأصيل مدخلاً ضرورياً لفهم طبيعة المخاطر السيبرانية التي ترافق التحول الرقمي السياحي، وأثرها على الثقة الرقمية واستدامة النشاط السياحي.

وانطلاقاً من ذلك، يُعالج هذا المحور ضبط المفاهيم الأساسية المرتبطة بموضوع الدراسة، من خلال تعريف الأمن السيبراني، وبيان مفهوم السياحة الرقمية، وتحديد المقصود بالجريمة الإلكترونية في السياق السياحي، فضلاً عن إبراز المركز القانوني للسائح باعتباره مستهلكاً رقمياً يستوجب حماية خاصة.

أولاً: تعريف الأمن السيبراني

يُقصد بالأمن السيبراني مجموعة التدابير القانونية والتنظيمية والتقنية الرامية إلى حماية الأنظمة الرقمية والبيانات المتداولة عبر شبكات الاتصال من مختلف صور الاعتداء الإلكتروني، بما يشمل الاختراق أو التعطيل أو النفاذ أو الاستخدام غير المشروع. ولا يقتصر

هذا المفهوم على حماية البنية التحتية الرقمية فحسب، بل يمتد ليشمل صون مصالح الأفراد والمؤسسات والحد من الآثار الاقتصادية والقانونية المترتبة عن التهديدات السيبرانية(سويلم، 2021).

ويُبرز هذا الطابع الشمولي للأمن السيبراني دوره الوقائي في تعزيز الثقة الرقمية وضمان استمرارية الأنشطة المعتمدة على الفضاء السيبراني، لاسيما في القطاعات الحيوية ذات البعد الاقتصادي والخدماتي، كالنشاط السياحي الرقمي.

1- البعد البشري والتوعوي كمرتكز قانوني للأمن السيبراني

يقوم الأمن السيبراني على بعدٍ بشري وتوعوي جوهري، يتمثل في تنمية الوعي الرقمي لدى المستخدمين وتعزيز ثقافة الاستخدام الآمن والمسؤول للتقنيات الحديثة، باعتبار أن العنصر البشري يُعدّ من أكثر نقاط الضعف عرضة للاستغلال في الهجمات السيبرانية. فمهما بلغت درجة تطور النظم التقنية، فإن السلوك غير الآمن للمستخدمين، كضعف كلمات المرور أو الوقوع في فخ التصيد الإلكتروني أو إساءة استخدام البيانات، يظل عاملاً حاسماً في نجاح الاعتداءات الإلكترونية. وعليه، تبرز أهمية برامج التكوين والتدريب المستمر، واعتماد سياسات داخلية واضحة للأمن المعلوماتي، بما يضمن رفع مستوى اليقظة الرقمية والحد من المخاطر المرتبطة بالأخطاء البشرية، خاصة في القطاعات المعتمدة على المعاملات الإلكترونية والخدمات الرقمية الحساسة(Commission, 2000).

2- التعاون الدولي كآلية قانونية لتعزيز الأمن السيبراني

يكتسب الأمن السيبراني بعداً دولياً وتعاونياً متزايد الأهمية، نظراً للطبيعة العابرة للحدود للفضاء السيبراني، حيث لم تعد التهديدات الرقمية محصورة في نطاق جغرافي محدد، بل تمتد آثارها عبر دول وأنظمة قانونية متعددة. ويستدعي هذا الواقع تنسيق الجهود بين الدول، وتعزيز التعاون الدولي من خلال تبادل المعلومات والخبرات، وتوحيد المعايير

القانونية والتقنية لمكافحة الجرائم السيبرانية، وهو ما أكدته اتفاقية بودابست بشأن الجريمة السيبرانية لسنة 2001، التي أرست إطارًا للتعاون الدولي في مجال مكافحة الجرائم المرتكبة عبر النظم المعلوماتية. كما يفرض هذا السياق اعتماد آليات دولية مشتركة للتصدي للهجمات الإلكترونية، بما يضمن حماية فعّالة للأنظمة المعلوماتية، ويعزز الثقة في البيئة الرقمية العالمية، لا سيما في القطاعات ذات الطابع العابر للحدود كالسياحة الرقمية والتجارة الإلكترونية. (Europe, 2025).

ثانياً: تعريف السياحة الرقمية

يقصد بالسياحة الرقمية توظيف التقنيات والمنصات الرقمية في تنظيم وتقديم الخدمات السياحية عبر مختلف مراحل الرحلة، بما يتيح إبرام المعاملات السياحية وتبادل البيانات والتفاعل بين السائح ومزوّدي الخدمات في بيئة رقمية مترابطة. ولا يقتصر هذا النمط على تحسين التجربة السياحية فحسب، بل يُنشئ علاقات قانونية رقمية جديدة تقوم على معالجة البيانات الشخصية، وإبرام العقود عن بُعد، وتحمل المخاطر السيبرانية. ومن ثم، تُعد السياحة الرقمية إطارًا وظيفيًا تتقاطع فيه الاعتبارات التقنية مع الحماية القانونية للسائح بوصفه مستهلكاً رقمياً، بما يفرض إعادة التفكير في آليات الأمن السيبراني والضمانات القانونية المصاحبة لها (Benyon, Quigley, O'Keefe, و Giuseppe, 2014).

1- البعد التقني والوظيفي للسياحة الرقمية

تعكس السياحة الرقمية نمطاً معاصراً لممارسة النشاط السياحي، يقوم على إدماج النظم المعلوماتية والتطبيقات الرقمية في إدارة العلاقة بين السائح ومقدمي الخدمات، بما يمكن من إنجاز مختلف العمليات السياحية ضمن فضاء إلكتروني متكامل. ويتجلى هذا التحول في الانتقال من النمط التقليدي إلى نموذج رقمي يعتمد على المعالجة الآنية للبيانات، وإبرام المعاملات التعاقدية عن بُعد، واستثمار الأدوات الذكية لتوجيه الاختيارات السياحية

وتكييفها وفق تفضيلات المستهلك. ولا يقتصر أثر هذه الرقمنة على تبسيط إجراءات النفاذ إلى الخدمات، بل يمتد ليعيد هيكلة آليات اشتغال المؤسسات السياحية، ويعزز قدرتها التنافسية، ويرسّخ الترابط الوظيفي بين مختلف المتدخلين ضمن منظومة رقمية تتميز بالمرونة والديناميكية. (Zhang و Szab، 2024).

2- التأسيس القانوني لحماية السائح الرقمي في سياق السياحة الرقمية المعاصرة»

لا تنحصر السياحة الرقمية في كونها مجرد تجسيد للتطور التقني في أساليب تقديم الخدمات السياحية، بل تمثل فضاءً قانونيًا مستحدثًا تُعاد فيه صياغة الروابط التعاقدية والالتزامات بين أطراف العلاقة السياحية، في إطار تنظيم قانوني جديد يتكيف مع التحولات الرقمية. ويؤدي اعتماد الوسائط الرقمية إلى نشوء علاقات قانونية قائمة على التعاقد الإلكتروني، والمعالجة الآلية للبيانات الشخصية، وتحمل المخاطر الرقمية الخاصة، وفي مقدمتها المخاطر السيبرانية الناجمة عن الاختراق أو الاستعمال غير المشروع للمعلومات. وفي هذا السياق، يبرز السائح الرقمي بوصفه مستهلكًا يتمتع بحقوق قانونية نوعية، تشمل ضمان أمن بياناته، وشفافية المعاملات، وسلامة الأداء الإلكتروني (William ، Basel ، Pam، و Namho، 2020) ومن ثم، تفرض السياحة الرقمية إعادة تقييم فعالية منظومة الأمن السيبراني والإطار القانوني المصاحب لها، بما يحقق التوازن بين متطلبات التحول الرقمي وحماية الحقوق القانونية للسائح الرقمي، ويضمن بيئة سياحية رقمية آمنة وموثوقة. (law، 2015).

ثالثًا: تعريف الجريمة الإلكترونية في السياحة الرقمية

تُعرف الجريمة الإلكترونية في سياق السياحة الرقمية على أنها كل سلوك غير مشروع يُرتكب عبر الوسائط أو النظم الرقمية ويستهدف المساس بالبيانات، المعاملات، أو الثقة الرقمية المرتبطة بالنشاط السياحي. ولا تنفصل هذه الجرائم عن مبدأ الشرعية الجنائية، إذ تقوم

على أفعال مجرّمة قانوناً(حسني، 1989)، غير أن تميزها يكمن في اعتمادها على الفضاء السيبراني كوسيط للارتكاب وما يترتب عن ذلك من تحديات في الكشف والتتبع وتحديد الاختصاص القضائي. وفي هذا الإطار، تتخذ الجريمة الإلكترونية صوراً متعددة؛ فقد يكون النظام المعلوماتي نفسه هدفاً للاعتداء، أو وسيلةً لارتكاب الجريمة، أو الإطار الذي يحدث فيه الضرر. وتنعكس هذه الجرائم مباشرة على أمن السائح الرقمي وسلامة معاملاته، كما تؤثر في الثقة الرقمية واستدامة النشاط السياحي، ما يستلزم تعزيز آليات الحماية القانونية والتقنية لمواجهة المخاطر السيبرانية.(المصري، 2010).

1- البعد المفاهيمي والتقني للجريمة الإلكترونية في السياحة الرقمية وحماية السائح الرقمي

تُشكّل الجريمة الإلكترونية في سياق السياحة الرقمية نمطاً خاصاً من السلوك الإجرامي غير المشروع، يعتمد على استغلال النظم المعلوماتية والوسائط الرقمية للإضرار بالمصالح المرتبطة بالنشاط السياحي. وتتجلّى خصوصيتها في اعتماد الفضاء السيبراني كبيئة ارتكاب، حيث قد يكون النظام المعلوماتي هدفاً للاعتداء، أو أداةً لتنفيذ الفعل الإجرامي، أو إطاراً تُستثمر فيه البيئة الرقمية لإحداث الضرر، سواء تعلق الأمر بالبيانات، المعاملات، أو الثقة الرقمية. ويترتب على هذا الطابع التقني تعقيد البنية الإجرامية من حيث وسائل الارتكاب وسرعة انتشار آثارها وصعوبة تتبعها، ما يجعلها تهديداً مباشراً لأمن السائح الرقمي وسلامة المعاملات السياحية المنجزة عبر الوسائط الإلكترونية، ويبرز الحاجة إلى تعزيز آليات الحماية القانونية والتقنية لضمان بيئة سياحية رقمية آمنة وموثوقة. (Haghani, Rajabifard, & Benny , 2025).

2- البعد القانوني والإجرائي للجريمة الإلكترونية وآليات حماية السائح الرقمي في السياحة الرقمية

لا تنفصل الجريمة الإلكترونية عن مبدأ الشرعية الجنائية، فهي قائمة على أفعال مجرّمة قانوناً، إلا أن طابعها الرقمي يفرض تحديات قانونية وإجرائية خاصة، تتجلى في صعوبة كشفها، وتتبع مرتكبيها، وإثبات أركانها، فضلاً عن تحديد الاختصاص القضائي الملائم، لا سيما في السياحة الرقمية العابرة للحدود. ويتربط على هذه الخصوصية آثار قانونية جسيمة على السائح الرقمي، سواء عبر التعدي على بياناته الشخصية، أو أمواله، أو حقوقه التعاقدية، بما ينعكس مباشرة على الثقة الرقمية واستدامة النشاط السياحي. ومن ثم، تظهر الحاجة إلى إعادة صياغة القواعد الجنائية التقليدية لتتماشى مع خصوصيات الجريمة الإلكترونية، مع تعزيز آليات التعاون القضائي الدولي، واعتماد وسائل قانونية وتقنية متكاملة تضمن حماية السائح الرقمي، وتردع الممارسات الإجرامية، وتدعم استقرار البيئة السياحية الرقمية. (خليفة سميّر و بعيرة ، 2024).

رابعا: تعريف السائح الرقمي كمستهلك إلكتروني وخصوصياته القانونية

يُقصد بالسائح بوصفه مستهلكاً رقمياً ذلك الشخص الذي يعتمد على الوسائط الرقمية والتطبيقات الإلكترونية في تخطيط رحلته السياحية، وحجز خدماتها، والدفع مقابلها، والتفاعل مع مقدميها، دون حضور مادي مباشر (نهلة، عبد الصادق، و عبد الحفيظ، 2021). وتتميّز هذه الصفة بكون السائح يمارس استهلاكه في فضاء افتراضي عابر للحدود، يقوم على الثقة الرقمية وتبادل البيانات الشخصية والمالية، مما يجعله أكثر عرضة للمخاطر السيبرانية. وفي هذا الإطار، لا يقتصر مفهوم السائح الرقمي على مجرد إبرام العقود الإلكترونية، بل يمتد ليشمل مختلف صور التفاعل الرقمي المرتبطة بالنشاط السياحي، وهو ما يضيف عليه خصوصية قانونية تستوجب حماية معززة، خاصة في ظل غياب تعريف تشريعي صريح له في القانون الجزائري، رغم إمكانية استيعابه ضمن مفهوم المستهلك الإلكتروني كما ورد في التشريع المنظم للتجارة الإلكترونية (السويدي و عباس محسن كرامشة ، 2025).

1- البعد المفاهيمي والوظيفي للسائح الرقمي: دوره في السياحة الرقمية وحماية

حقوقه

يُفهم السائح الرقمي على أنه الفرد الذي يعتمد على الوسائط الرقمية، التطبيقات، والمنصات الإلكترونية في تنظيم رحلته السياحية بكامل مراحلها، بدءًا من البحث عن الخدمات وحجزها والدفع مقابلها، وصولًا إلى التفاعل مع مقدميها ومتابعة الخدمات بعد تنفيذها، دون الحاجة إلى حضور مادي مباشر. وتتم ممارسة هذه العلاقة الاستهلاكية ضمن فضاء افتراضي عابر للحدود الجغرافية، يركز على الثقة الرقمية وتبادل المعلومات الشخصية والمالية، ما يجعل السائح الرقمي عنصرًا فاعلاً ومؤثرًا ضمن منظومة سياحية رقمية مترابطة. ولا يقتصر مفهوم السائح الرقمي على مجرد إبرام العقود الإلكترونية، بل يشمل جميع أشكال التفاعل الرقمي المرتبطة بالنشاط السياحي، بما في ذلك استخدام تطبيقات التقييم، خدمات الدعم الإلكتروني، ومنصات الوساطة الرقمية، الأمر الذي يزيد من حجم البيانات المتداولة ويضاعف تعرضه للمخاطر السيبرانية. ومن ثم، يستلزم هذا الواقع اعتماد حماية قانونية وأمنية متكاملة لضمان حقوق السائح الرقمي وصيانة سلامة البيئة السياحية الرقمية (Buhalis & Law, 2008).

2- البعد القانوني للسائح الرقمي: الحاجة إلى حماية معززة وضمان الحقوق في السياحة

الرقمية

اكتسب السائح الرقمي، بوصفه مستهلكًا إلكترونيًا، وضعًا قانونيًا خاصًا يستوجب تعزيز حماية حقوقه، نظرًا للفجوة التي قد تنشأ في موازين القوة التعاقدية ضمن البيئة الرقمية، وصعوبة التحقق من هوية مزودي الخدمات، فضلًا عن المخاطر المصاحبة لأمن البيانات والمعاملات الإلكترونية. وتصبح هذه الخصوصية القانونية أكثر وضوحًا في ظل غياب تعريف تشريعي محدد للسائح الرقمي في القانون الجزائري، رغم إمكانية

إدراجه ضمن مفهوم المستهلك الإلكتروني كما ورد في التشريعات المنظمة للتجارة الإلكترونية، مثل القانون 05-18 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 المتعلق بالتجارة الإلكترونية، الجريدة الرسمية العدد 28، المؤرخة 30 شعبان 1439 الموافق 16 مايو سنة 2018، ومن ثم تبرز الحاجة إلى تطوير وتفعيل قواعد حماية المستهلك الرقمي وتكييفها وفق خصوصيات النشاط السياحي الرقمي، بما يكفل صون حقوق السائح، وتعزيز الثقة في البيئة الرقمية، ودعم استدامة النموذج السياحي الرقمي. (حمزة وعزايز ، 2022)،

المحور الثاني: التحديات السيبرانية وآثارها على أمن المعلومات وحماية السائح الرقمي
أسفر التوسع المتسارع في رقمنة النشاط السياحي عن اعتماد متزايد على المنصات الإلكترونية، تطبيقات الحجز، أنظمة الدفع الرقمي، وفضاءات التواصل الاجتماعي، ما أسهم في تحسين جودة الخدمات السياحية وتعزيز تجربة السائح. غير أن هذا التحول الرقمي، وبقدر ما يوفره من مزايا، أوجد بيئة خصبة لظهور تهديدات سيبرانية متنامية تستهدف المعطيات الشخصية، العمليات المالية، والبنى المعلوماتية للمنشآت السياحية. ويغدو استيعاب طبيعة هذه المخاطر شرطاً جوهرياً لتصميم آليات حماية فعالة (محمد، 2024)، لا سيما في ظل تصاعد أنماط الهجمات الإلكترونية، من قبيل التصيد الاحتيالي، الاختراق غير المشروع لقواعد البيانات، ونشر البرمجيات الخبيثة، وهي ممارسات تنعكس مباشرة على أمن المعلومات وتهدد خصوصية السائح الرقمي وثقته في الفضاء السياحي الإلكتروني (حكيم، 2021).

أولاً: التهديدات السيبرانية للبنية الرقمية السياحية وأثرها على أمن المعلومات وثقة السائح الرقمي

عدّ أمن المعلومات في القطاع السياحي الرقمي من أكثر المجالات عرضة للاستهداف السيبراني، خاصة مع التوسع في منصات الحجز الإلكتروني، أنظمة إدارة الفنادق، وتطبيقات السفر الذكية. فقد أصبحت هذه البنى الرقمية بيئة جاذبة للهجمات السيبرانية، خصوصًا خلال مواسم الذروة السياحية، حيث تتكثف محاولات اعتراض البيانات الحساسة أو النفاذ غير المشروع إلى قواعد البيانات بغرض الاستيلاء على المعطيات الشخصية والمالية للسائح (Nguyen, Hung Nguyen, Dung Tien, & Duc , 2022). كما تشمل الهجمات تعطيل المنصات عبر حجب الخدمة، ما يؤدي إلى توقف الخدمات، تكبد خسائر مالية، والإضرار بسمعة المؤسسات والوجهات السياحية. وتتفاقم خطورة هذه التهديدات بفعل انتشار البرمجيات الخبيثة وهجمات برامج الفدية التي تستهدف أنظمة التسيير الإلكتروني، مسببة شل العمليات التشغيلية أو فقدان البيانات/تشفيرها. كما تواجه المنصات السياحية مخاطر إضافية من استغلال الثغرات التقنية والتلاعب بالمحتوى الرقمي باستخدام الذكاء الاصطناعي (Deepfake)، ما يهدد مصداقية المعلومات السياحية وصورة الوجهات. يكشف هذا الواقع عن تنوع وتعقيد التهديدات السيبرانية، ويبرز الحاجة الملحة إلى اعتماد منظومات أمنية متقدمة، قادرة على الرصد الاستباقي للهجمات وحماية حقوق السائح الرقمي وضمان استمرارية الخدمات وتعزيز الثقة في الفضاء السياحي الرقمي. (غيش، 2022).

ثانياً: آليات الاستهداف السيبراني الموجّه للسائح الرقمي في البيئة السياحية الذكية
أضحى السائح الرقمي يشكّل هدفاً مباشراً لعمليات الاستهداف السيبراني الموجّه، نتيجة تعاظم اعتماده على المنصات الذكية والتطبيقات الرقمية في مختلف مراحل الرحلة السياحية، من التخطيط والحجز إلى الاستفادة من الخدمات الإلكترونية أثناء التنقل والإقامة. وقد أسهم التطور المتسارع في تقنيات القرصنة والاحتيال الرقمي في بروز أنماط

هجومية مبتكرة تقوم أساسًا على استغلال الثقة الرقمية التي يمنحها السائح للأنظمة والمنصات السياحية، وما يرافق ذلك من تبادل مكثف للبيانات الشخصية والمالية. وتُعدّ الهجمات الموجهة ضد منصات الحجز الإلكتروني من أكثر صور هذا الاستهداف شيوعًا، حيث تُستغل مواسم الذروة السياحية لتنفيذ عمليات اعتراض بيانات الدفع، أو تعطيل الخدمات الرقمية، بما يؤدي إلى اضطراب المنصات ويُفضي إلى مساس مباشر بحق السائح في حماية معطاته الشخصية وأمنه المالي (Gharibi, 2011) ولا يقتصر الاستهداف السيبراني للسائح الرقمي على الوسائل التقنية التقليدية، بل يمتد إلى أساليب احتيالية متقدمة قائمة على الهندسة الاجتماعية الرقمية، من خلال رسائل إلكترونية أو تطبيقات مزيفة تحاكي واجهات خدمات سياحية معروفة، بهدف دفع السائح إلى الإفصاح الطوعي عن بياناته الشخصية أو المالية. كما ساهم الانتشار المتزايد لتقنيات التزييف العميق (Deepfake) والتصيد الاحتيالي الذكي (Smart Phishing) في تعزيز قدرة المهاجمين على إنتاج محتويات رقمية عالية الإقناع يصعب تمييزها عن المصادر الأصلية، ما يؤدي إلى ارتفاع معدلات الاحتيال والسرقة الرقمية (الناغي و محمد محروس الناغي، 2024). وإلى جانب ذلك، تشهد البيئة السياحية الرقمية توسعًا في ممارسات تتبع البيانات واستغلالها بطرق غير مشروعة، سواء لأغراض مالية لاحقة أو لإعادة بيعها في أسواق البيانات غير القانونية. ويكشف هذا التطور النوعي في أساليب الهجوم عن تحدٍّ مباشر لأمن معلومات السائح الرقمي وخصوصيته، مما يستلزم تعزيز الأطر القانونية، وتطوير آليات الحماية التقنية المتكاملة، لضمان صون الحقوق الرقمية للسائح وتعزيز ثقته في المنظومة السياحية الرقمية.

المحور الثالث: الحوكمة الرقمية للسياحة: استراتيجيات الأمن السيبراني وضمان

حقوق السائح الرقمي

ترتكز استراتيجيات الأمن السيبراني في السياحة الرقمية على إرساء منظومة متكاملة متعددة الطبقات تهدف إلى حماية المنصات والخدمات الإلكترونية من مختلف التهديدات السيبرانية المتجددة، عبر توظيف تقنيات حماية متقدمة مثل التشفير، أنظمة كشف التسلل، والنسخ الاحتياطي، بالإضافة إلى اعتماد سياسات أمنية واستراتيجية حوكمة دقيقة تتماشى مع طبيعة المخاطر الرقمية. وتسعى هذه الاستراتيجيات إلى ضمان سلامة البنية المعلوماتية والمعاملات الرقمية، وصون المعطيات الشخصية والمالية للسائح الرقمي، مع تعزيز الثقة في البيئة السياحية الرقمية وتوفير تجربة سياحية آمنة ومستقرة وموثوقة، كما تؤكد على الامتثال للأطر القانونية والتنظيمية ذات الصلة بحقوق المستهلك الرقمي.

أولاً: بروتوكولات وإجراءات الأمن الرقمي لحماية السائح

تمثل حماية البيانات الشخصية والمالية للسائح الرقمي ركيزة أساسية لضمان أمنه وتعزيز ثقته في المنصات السياحية الرقمية، كما تشكل عاملاً جوهرياً في الحفاظ على سمعة الوجهات السياحية وتقليل المخاطر المالية المحتملة. وتستند هذه الحماية إلى منظومة متكاملة من بروتوكولات وإجراءات الأمن الرقمي، لا سيما في عمليات الحجز والدفع الإلكتروني، من خلال اعتماد تقنيات تشفير متقدمة مثل بروتوكولات SSL، وتطبيق آليات التحقق متعدد العوامل MFA، بما يضمن سرية المعاملات ويحول دون الوصول غير المصرح به إلى المعلومات الحساسة. وتبرز أهمية هذه الإجراءات في الحد من الاختراقات الإلكترونية وحماية مصالح السياح والمؤسسات على حد سواء، مما يعزز الثقة الرقمية ويضمن استمرارية العمليات السياحية بأمان. (إيمان، 2022).

ولا يقتصر الأمن الرقمي على الجوانب التقنية فحسب، بل يشمل البعد البشري، حيث يمثل تكوين وتدريب العاملين في القطاع السياحي على رصد التهديدات السيبرانية وأساليب الاختيال الرقمي ركيزة أساسية لتعزيز الجاهزية الأمنية للمؤسسات السياحية. ويسهم هذا

النهج في رفع مستوى الوعي الوقائي، وتقوية قدرة المؤسسات على الاستجابة الفورية للهجمات الإلكترونية، والحد من الآثار السلبية المحتملة على بيانات السائح. كما تلعب المراجعات الدورية للأنظمة المعلوماتية وإجراء اختبارات الاختراق (Penetration Testing) دورًا محوريًا في الكشف الاستباقي عن الثغرات التقنية ومعالجتها قبل أن تستغلها الجهات الخبيثة، بما يعزز استقرار المنصات الرقمية ويحافظ على ثقة المستخدمين. (Zhang, Ju, & Xiaoqi, 2025). ويضاف إلى ذلك أهمية اعتماد سياسات فعالة لإدارة البيانات وتحليل التدفقات السياحية بطريقة آمنة، بما يضمن حماية المعلومات في مختلف مراحل التخطيط والتنفيذ السياحي، ويعزز في الوقت نفسه استدامة الوجهات السياحية وجودة الخدمات المقدمة (Soualah-Alila, Faucher, Frédéric, Coustaty, & Doucet, 2015) وبذلك، يسهم تطبيق بروتوكولات وإجراءات الأمن الرقمي في إرساء بيئة سياحية رقمية آمنة وموثوقة، تكفل حماية خصوصية السائح الرقمي، وتدعم استدامة النشاط السياحي، وتعزز ثقة المستهلك في المنظومة الرقمية للقطاع السياحي.

ثانيًا: حماية المنصات الرقمية والأمن السيبراني لضمان استدامة وجاذبية الوجهات السياحية

تشكل منصات الحجز والخدمات السياحية الرقمية البنية الأساسية للتجربة السياحية في الفضاء الرقمي، ما يجعلها من أكثر الأهداف تعرضًا للهجمات السيبرانية بمختلف أشكالها. ولمواجهة هذه المخاطر، تبرز أهمية اعتماد استراتيجيات أمنية شاملة، تشمل الصيانة الدورية للأنظمة والتحديث المستمر لسد الثغرات التقنية المحتملة، إلى جانب استخدام الجدران النارية (Firewalls) وأنظمة كشف ومنع التسلل (IDS/IPS) لرصد الأنشطة غير المشروعة والتصدي لها قبل أن تؤثر على سير العمليات والخدمات (Alkasassbeh, 2017). ويُعد اللجوء إلى اختبارات الاختراق الدورية (Penetration Testing) أداة فعالة لتقييم

مدى متانة المنصات الرقمية وقدرتها على مقاومة الهجمات السيبرانية المتقدمة، بما يضمن استمرارية الخدمات الإلكترونية ويحدّ من المخاطر التي قد تهدد أمن السائح الرقمي. ولا ينفصل الأمن السيبراني في هذا السياق عن متطلبات استدامة وجاذبية الوجهات السياحية، إذ تسهم حماية البيانات وإدارة التدفقات السياحية الرقمية بصورة آمنة في الحفاظ على الموارد السياحية وتعزيز ثقة السائح في الوجهة المختارة. كما تتمتع الوجهات التي تعتمد منظومات أمن رقمي متطورة بقدرة أكبر على تعزيز تنافسيتها الاقتصادية وجاذبيتها على المستويين الإقليمي والدولي. ومن خلال الاستثمار الاستراتيجي في الأمن السيبراني، يمكن تحويل التحديات الرقمية إلى فرص لتحسين جودة الخدمات السياحية، وتوفير تجربة سفر آمنة وموثوقة، بما يدعم مكانة الوجهة السياحية ويضمن تحقيق تجربة متكاملة ومستدامة للسائح الرقمي(الصادق، 2025).

ثالثاً: التوعية السيبرانية كآلية وقائية لتعزيز أمن السائح الرقمي وحماية البيانات

تلعب التوعية والتثقيف السيبراني دوراً جوهرياً في تعزيز حماية السائح الرقمي، إذ يسهم رفع مستوى الوعي بالمخاطر الإلكترونية في الحد من احتمالات تعرضه للهجمات السيبرانية المختلفة. وتستند هذه المقاربة إلى اعتماد برامج وحملات توعوية موجهة، تهدف إلى تعريف السائح بطبيعة التهديدات الرقمية الشائعة، مثل الاحتيال الإلكتروني (Phishing)، والتزييف الرقمي العميق (Deepfake)، وجرائم سرقة البيانات المالية(غنية، 2024)، بما يمكنه من التمييز بين السلوكيات الرقمية الآمنة والممارسات المحفوفة بالمخاطر. وتشمل هذه الجهود أيضاً تزويد السائح بإرشادات عملية لتأمين أجهزته الذكية وتعزيز ممارسات الحماية الذاتية، لا سيما فيما يتعلق بتفادي مشاركة البيانات الحساسة مع مصادر غير موثوقة أو عبر شبكات غير آمنة. كما تضطلع المؤسسات السياحية بدور تكميلي من خلال توفير أدلة إجرائية واضحة تحدد سبل التصرف الواجب اتباعها عند التعرض لأي تهديد رقمي، بما

يضمن سرعة الاستجابة وتقليص الأضرار المحتملة. ويسهم هذا الإطار التوعوي في تعزيز ثقة السائح في المنصات السياحية الرقمية، ويدعم بناء بيئة سياحية رقمية آمنة تقوم على الاستخدام الواعي والمسؤول للتقنيات الحديثة (بوخضرة، 2022).

خاتمة

يُظهر التحول الرقمي المتسارع في القطاع السياحي العربي، رغم الفرص الكبيرة التي يوفرها لتطوير الخدمات وتحسين تجربة السائح، تزايداً مستمراً في التهديدات السيبرانية التي تستهدف كلاً من المستهلك الرقمي والمنصات السياحية. وتشير نتائج هذا البحث إلى أن الأمن السيبراني أصبح عنصراً أساسياً لا غنى عنه لضمان الثقة الرقمية، واستمرارية تقديم خدمات سياحية موثوقة، وتعزيز استدامة الوجهات. كما يتضح أن حماية السائح وإدارة البيانات والتدفقات السياحية بشكل آمن تمثل ركائز استراتيجية لتطوير نموذج سياحي رقمي قادر على مواجهة المخاطر وتحويلها إلى فرص للابتكار والتحسين المستمر، بما يسهم في تعزيز تنافسية الوجهات وجاذبيتها على المستويين الإقليمي والدولي، ويضمن تجربة سياحية رقمية آمنة ومستدامة.

نتائج الدراسة

- تشير النتائج إلى تزايد المخاطر السيبرانية التي تواجه كلاً من السائح الرقمي والمنصات السياحية الرقمية نتيجة الاعتماد المتزايد على التطبيقات الذكية والحجز الإلكتروني، مما يستلزم تبني آليات حماية أكثر تطوراً وفاعلية.
- يتضح أن الأمن السيبراني أصبح شرطاً أساسياً لاستدامة الوجهات السياحية، عبر حماية البيانات الحساسة، وتعزيز الثقة الرقمية لدى المستخدمين، ودعم التنافسية في بيئة السياحة الرقمية المتسارعة.

- يشكل تحسين الحوكمة الرقمية وتطوير مهارات العاملين في القطاع السياحي ركيزة استراتيجية لمعالجة نقاط الضعف التقنية والبشرية، وضمان إدارة آمنة للتدفقات السياحية، بما يساهم في تحسين جودة التجربة السياحية وتعزيز الاستدامة الرقمية للوجهات.
- تكامل تقنيات الذكاء الاصطناعي مع آليات الأمن السيبراني يتيح توقع الهجمات قبل حدوثها، ويضع أسسًا لنظام دفاع استباقي ذكي مخصص للقطاع السياحي، مما يقلل من فرص الاستغلال الرقمي ويُحسّن استجابة المؤسسات.
- استخدام منصات تفاعلية للتثقيف السيبراني الموجه للسائح الرقمي يعزز قدرة المستهلك على اتخاذ قرارات آمنة، ويخلق نموذجًا جديدًا للمشاركة التفاعلية في الأمن الرقمي، مما يحوّل السائح من طرف مستهلك فقط إلى فاعل نشط في حماية نفسه والمنظومة الرقمية.

التوصيات

- تعزيز البنية التحتية للأمن السيبراني: ينبغي تبني أنظمة تشفير متقدمة، وتفعيل آليات التحقق متعدد العوامل، وإجراء تحديث دوري للمنصات الرقمية لضمان مقاومة الهجمات المتطورة والحفاظ على سرية البيانات وحماية المعاملات السياحية الإلكترونية.
- وضع استراتيجية وطنية متكاملة لحماية السائح الرقمي: تشمل هذه الاستراتيجية تطوير بروتوكولات واضحة للاستجابة للحوادث السيبرانية، وتوحيد معايير حماية البيانات على مستوى القطاع السياحي، مع رصد مستمر للتهديدات وتقييم المخاطر بشكل دوري.

- رفع مستوى الوعي الرقمي للعاملين والسياح: من خلال تنفيذ برامج تدريبية دورية للموظفين، وإطلاق حملات توعية موجهة للسائح حول أساليب الاحتيال الرقمي وطرق حماية بياناته الشخصية والمالية، مما يساهم في تعزيز ثقافة الأمن الرقمي لدى جميع الأطراف.
- تعزيز التعاون بين القطاعين العام والخاص: عبر إنشاء منصات مشتركة لرصد التهديدات الرقمية، وتبادل المعلومات والخبرات بين الجهات الأمنية، والمؤسسات السياحية، وتطوير آليات استجابة جماعية تمكن من التصدي السريع للهجمات وحماية المنظومة الرقمية بشكل فعال.
- توظيف التقنيات الذكية لمراقبة المخاطر والاستجابة المبكرة: مثل استخدام الذكاء الاصطناعي وتحليل البيانات للتنبؤ بالهجمات السيبرانية وتفعيل آليات دفاع استباقية، مما يقلل من احتمالات الاختراق ويعزز ثقة السائح الرقمي في المنصات السياحية.

قائمة المراجع

- Alkasassbeh, M. (2017, décembre 27). *An empirical evaluation for the intrusion detection features based on machine learning and feature selection method*. Retrieved January 22, 2026, from Cornell University:
https://arxiv.org/abs/1712.09623?utm_source=chatgpt.com
- Benyon, D., Quigley, A., O’Keefe , B., & Giuseppe, R. (2014). Presence and digital tourism. *AI & SOCIETY* , 29 (4), pp. 521–529.
- Buhalis, D., & Law, R. (2008, August). Progress in Information Technology and Tourism Management: 20 Years on and 10 Years After the Internet—The State of eTourism Research. (B. H. University, Ed.) *Tourism Management*, 29(4), pp. 609-623.
- Commission, I. O. (2000). *ISO/IEC 27001:2022 — Information security management systems — Requirements*, 3. Retrieved Janvier 21, 2026, from ISO:
<https://www.iso.org/standard/27001>
- Europe, C. o. (2025, July). *The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols*. Retrieved janvier 21, 2026, from Council of Europe/Cybercrime:
<https://www.coe.int/en/web/cybercrime/the-budapest-convention>
- Gharibi, W. (2011, Jun 4). *Studying and Classification of the Most Significant Malicious Software*. Retrieved January 22, 2026, from Cornell University : <https://arxiv.org/abs/1106.0853>
- Haghani, M., Rajabifard, A., & Benny , C. (2025, May 5). *What is a ‘smart city’ and why should we care? It’s not just a buzzword*. Retrieved January 21, 2026, from The Conversation:

- <https://theconversation.com/what-is-a-smart-city-and-why-should-we-care-its-not-just-a-buzzword-255419>
- law, E.-L. t. (2015, 11 25). *Directive (EU) 2015/2302 of the European Parliament and of the Council of 25 November 2015 on package travel and linked travel arrangements, amending Regulation (EC) No 2006/2004 and Directive 2011/83/EU of the European Parliament and of the Council and r.* Consulté le Janvier 22, 2026, sur European Union: <https://eur-lex.europa.eu/eli/dir/2015/2302/oj/eng>
- Nguyen, T. T., Hung Nguyen, Q., Dung Tien, N., & Duc , T. (2022, Octobre 25). Deep learning for deepfakes creation and detection: A survey. *Computer Vision and Image Understanding*, 233(103525), p. 103525.
- Pam, L., Basel , H., William, C., & Namho, C. (2020). Smart Tourism City. *Developments and Transformations*, 12(10), pp. 39-58.
- Soualah-Alila, F., Faucher, C., Frédéric , B., Coustaty, M., & Doucet, A. (2015, November 15). *Applying Semantic Web Technologies for Improving the Visibility of Tourism Data*. Retrieved January 22, 2026, from Cornell University: <https://arxiv.org/abs/1511.04717>
- Zhang, W., Ju , X., & Xiaoqi , L. (2025, May 25). *Penetration Testing for System Security: Methods and Practical Approaches*. Retrieved January 22, 2026, from Cornell University : <https://arxiv.org/abs/2505.19174>
- Zhang, Y., & Szab, Z. (2024, May). Digital Transformation in the Tourism Industry: A Comparative Literature Review. *Advances in Economics Management and Political Sciences*, 72(1), pp. 166-179.
- العيداني مُجَّد. (14 1, 2024). التهديدات السيبرانية وجرائم المعلومات. (المركز الجامعي الشريف بوشوشة، المحرر) مجلة الاجتهاد للدراسات القانونية والاقتصادية، 13(1)، الصفحات 15-37.
- دار العدالة :القاهرة.الجرائم المعلوماتية و الرقمية للحاسوب و الانترنت. (2010). ي. المصري

- بن جروة حكيم. (2021). واقع السياحة الالكترونية في الجزائر و دورها في ترويج المنتجات السياحية. (جامعة قاصدي مرباح، المحرر) 24(1)، الصفحات 1311-1327.
- دارالنهضة العربية :القاهرة. (éd. 6)شرح قانون العقوبات القسم العام. (1989). ن. م. وحسني خلفه سمير، و آمال بعيرة . (20 12, 2024). الحماية الجزائية لوسائل الدفع الإلكتروني. (جامعة محمد البشير الإبراهيمي، المحرر) مجلة حقوق الإنسان والحريات العامة، 9(2)، الصفحات 235-268.
- د.عادل عبد الصادق. (الخميس، 20 فبراير , 2025). الامن السيبراني والاقتصاد في العصر الرقمي. تاريخ الاسترداد 22 جانفي, 2026، من المركز العربي لبحاث الفضاء الالكتروني/الدوريات - قضايا استراتيجية: https://accronline.com/article_detail.aspx?id=42194
- درناني ايمان. (Juin, 2022 18). دور المعاملات الرقمية و تطبيقات الدفع الالكتروني في تنمية السياحة في الجزائر. مداخلة مقدمة للمشاركة في نداعيات الملتقى الدولي الافتراضي: البيانات الضخمة و الاقتصاد الرقمي كآلية لتحقيق الاقلاع الاقتصادي في الدول النامية " الفرص، التحديات و الافاق " . الوادي، جامعة الشهيد حمة لخضر، الجزائر: كلية العلوم الاقتصادية و التجارية و علوم التسيير.
- 21, 2026, sur Consulté le 17 نوفمبر 2021). أ. س. وسويلم :موضوع اكبر موقع عربي بالعالم
https://mawdoo3.com/%D9%85%D9%81%D9%87%D9%88%D9%85_%D8%A7%D9%84%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A
- عباس غنية. (2024 , 12 30). الجريمة الإلكترونية في البيئة الرقمية ومدى تأثيرها على الجريمة المنظمة العابرة للحدود الوطنية. المجلة الجزائرية للسياسة العامة ، 12(3)، الصفحات 97-100.
- عز الدين غبش. (30 افريل, 2022). حماية المستهلك الإلكتروني في ظل الجرائم السيبرانية. (جامعة الشهيد حمة لخضر، المحرر) المجلة الدولية للتحويلات القانونية و السياسية، 1(1)، الصفحات 74-113.
- م.د. علي خيون كاطع السويدي، و م. جيهان عباس محسن كرماشة . (18 6, 2025). الحماية القانونية للمستهلك من مضار الذكاء الاصطناعي. (الجامعة الاسلامية /كلية القانون، المحرر) مجلة المعهد (20)، الصفحات 911-961.
- مريم بوخضرة. (2022). التحول الرقمي و رقمنة القطاع السياحي ودورها في تفعيل الاستثمار السياحي في المملكة العربية السعودية/ ل - Conference: ملتقى علمي وطني حول: الاستثمار السياحي

كخيار استراتيجي لتحقيق التنمية المستدامة يومي: الواقع و المأمول. ملتقى علمي وطني حول:
الاستثمار السياحي كخيار استراتيجي لتحقيق التنمية المستدامة. سوق اهراس/ الجزائر: جامعة محمد
الشريف بالمسعدية .

مزيان حمزة، و جلال عزايز . (2022). أثر استخدام تطبيقات التسويق السياحي الالكتروني على سلوك
المستهلك السائح. (جامعة حسية بن بوعلي، المحرر) مجلة الدراسات الاقتصادية المعاصرة، 7(1)،
الصفحات 38-50.

ولاء محمد محروس الناعي، و ياسر محمد محروس الناعي. (2024). إدراك مستخدمي مواقع التواصل الاجتماعي
لتهديدات التزييف العميق "Deep Fake" وعلاقته باستخدامهم الآمن لتلك المواقع. (قسم الإعلام
بكلية التربية النوعية- جامعة بورسعيد، المحرر) المجلة العلمية لبحوث الصحافة، 2022 (24)،
الصفحات 383-425.

يوسف نحلة، عبد الوهاب عبد الصادق، و سماح عبد الحفيظ. (ديسمبر، 2021). تأثير التحول الرقمي على
القدرة التنافسية والقيمة المضافة للقطاع السياحي. (المعهد العالي للدراسات النوعية، المحرر) مجلة اتحاد
الجامعات العربية للسياحة و الضيافة، 21(3)، الصفحات 233-271.