Turismo y ciberseguridad: riesgos, amenazas y oportunidades

Enrique Ávila Gómez

Metaversos, experiencias virtuales, teletrabajo, sensorización, inteligencia artificial... Términos extraños para comenzar un artículo relacionado con el turismo y la ciberseguridad. Más con lo primero que con lo segundo, dado que el turismo es, fundamentalmente, una experiencia humana analógica, a la que es difícil conectar, de forma directa, con el dominio del Ciberespacio.

Sin embargo, el modelo en el que desarrollamos nuestra actividad como sociedad supuestamente avanzada se caracteriza, entre otras cosas, por su complejidad. Una complejidad estructural, en un modelo de capas superpuestas, que predetermina toda actividad humana generando riesgos y amenazas sinfín y, por supuesto, oportunidades que podemos aprovechar para seguir avanzando. Una complejidad que no podríamos intentar controlar sin el uso masivo de tecnología. De tecnología interconectada en una red compuesta por trillones de nodos y que genera petabytes de información cada minuto, a nivel global.

Este modelo, por supuesto, impacta sobre todas las actividades productivas que, como especie, desarrollamos en este ecosistema único y globalizado. También en un sector, el turístico que, en nuestro país, representa entre 75.000 y 150.000 millones de euros[1], lo que viene a ser, si tomamos los datos de la prepandemia, aproximadamente, entre el 10 y el 15 % de toda nuestra actividad productiva.

Con estos datos no podemos tener ninguna duda: hemos de proteger este sector productivo, estratégico para nuestro país, que, además, se desarrolla en un entorno fuertemente competitivo y al que impacta una situación sociosanitaria que modificará completamente el escenario de desarrollo del mismo en los próximos años.

Ha transcurrido mucho tiempo y se han producido muchos acontecimientos desde aquellos primeros balbuceos, en los años sesenta del pasado siglo, de un modelo turístico basado en la excelencia de nuestro clima, en los precios asequibles y en nuestra necesidad de generar recursos para avanzar como país.

En los años transcurridos se han producido revoluciones culturales y tecnológicas que están transformando un sector que ha de ser cada día más eficiente y orientado a satisfacer a un cliente más exigente con los servicios que se le prestan durante un periodo vacacional o un viaje de negocios para ser competitivo en un mercado global.

Por esas razones y otras muchas conexas, ha sido necesario acometer un ambicioso y masivo programa de despliegue de tecnología en el sector que, sin duda, impulsa elementos tales como la eficiencia logística, la calidad de los servicios prestados o, últimamente, la seguridad sanitaria de quienes deciden visitarnos.

La apuesta-país orientada a aprovechar al máximo las oportunidades que ofrece el uso intensivo de tecnologías en la mejora de la calidad de los servicios prestados, así como en el análisis de los

datos obtenidos nos ha permitido desarrollar nuevas propuestas de servicios turísticos que permitan atraer a nuevos visitantes, preferentemente de mayor poder adquisitivo.

Sirva como ejemplo de lo antedicho el desarrollo de la denominada Red de Destinos Inteligentes[2], liderada por la Secretaría de Estado de Turismo, cuya definición y objetivos pueden obtenerse de la página Web de SEGITTUR:

> Destino Turístico Inteligente es un destino turístico innovador, consolidado sobre una infraestructura tecnológica de vanguardia, que garantiza el desarrollo sostenible del territorio turístico, accesible para todos, que facilita la interacción e integración del visitante con el entorno e incrementa la calidad de su experiencia en el destino y mejora la calidad de vida del residente.

Sostenibilidad, innovación, tecnología, integración..., todo ello orientado a mejorar la experiencia del visitante, son objetivos estratégicos de esta iniciativa.

La introducción de tecnología en los procesos de negocio, como ya sabemos, supone generar un amplio conjunto de nuevas oportunidades de negocio en cualquier sector productivo. Por supuesto, también en el sector turístico, pero todos somos conscientes ya de que el uso de la tecnología también provoca la aparición de riesgos y amenazas asociados que hemos de ser capaces de detectar, evaluar y mitigar mediante las inversiones necesarias.

Entender esto es fundamental, a pesar de la invaluabilidad de los activos que han de protegerse, frecuentemente no materiales, ya que éstos forman parte de los procesos de negocio y su pérdida, incluso parcial, puede generar enormes pérdidas e, incluso, la expulsión del mercado de forma permanente, de la empresa afectada.

La ciberseguridad, por tanto, se transforma en un elemento estructural del modelo de negocio en el sector turístico una vez se ha optado (y no hay alternativa viable), por la introducción masiva de la tecnología en los procesos logísticos, de servicio y de toma de decisión, más aún en un escenario de hiperconectividad, en el que nuestro negocio no constituye una isla desierta sino un nodo, más o menos importante, de una red extensa y compleja en la que una amenaza en cualquier nodo puede suponer la extensión de la misma al resto de la red.

Uno de los elementos estructurales que modulan el valor de un determinado destino turístico es, sin duda, la seguridad. Hasta hace poco, hemos conectado esta percepción con la seguridad física de nuestros visitantes. Afortunadamente, vivimos en un país seguro en el que nuestras Fuerzas y Cuerpos de Seguridad cumplen, de forma impecable, el objetivo de proteger y servir a la ciudadanía y a todas aquellas personas que nos visitan.

Sin, por supuesto, dejar de seguir apostando por el valor añadido que genera la seguridad física de las personas que nos visitan, hemos de adaptar el concepto para que encaje en el dominio del ciberespacio. Un teatro de operaciones en el que el Estado dispone de posibilidades de acción mucho más limitadas, al tratarse de un dominio caracterizado por su aterritorialidad en la aplicación de las leyes.

Si a esto añadimos el hecho de que la asimetría de recursos necesaria para causar un daño a una empresa u organización o la comisión de un ilícito penal contra las personas, es desproporcionado, esto es, que con pocos recursos puedes causar un gran daño, podemos dibujar un escenario de riesgo que sólo puede ser mitigado con inversiones adecuadas en la protección de los activos tecnológicos asociados al modelo de negocio turístico.

Pensemos en un ataque de guerra económica contra el sector o de inteligencia competitiva contra uno de los actores del mismo: La

interrupción del servicio de recepción y acogida de los clientes de un grupo hotelero por un ataque *ramsonware*. Se trata de un vector de ataque nada complejo de ejecutar y cuyas consecuencias económicas y reputacionales resultarían gravísimas y gravosas para la empresa.

¿Cómo ha sido posible? ¿De qué herramientas de protección nos habíamos dotado? ¿Habíamos concienciado, formado y entrenado a nuestro personal para detectar un ataque de estas características? ¿Disponíamos de algún centro o política de respaldo de la información para la recuperación de la información afectada? ¿Habíamos diseñado y comprobado el funcionamiento de planes de contingencia para mitigar el daño, tanto al cliente como a la propia empresa? Estas son, entre otras muchas, la cuestiones a las que ha de hacer frente un Departamento de Cumplimiento Normativo en Ciberseguridad, en cooperación con los Departamentos de Ciberseguridad correspondientes, de una gran empresa del sector o por parte de un servicio mutualizado para los pequeños operadores, con menores posibilidades de disponer de recursos propios para mitigar estos riesgos y amenazas.

Pero el escenario propuesto no es sino un modesto ejemplo de lo que puede llegar a acontecer. Podemos diseñar escenarios en los que el impacto puede ser más grave que el anteriormente descrito. Escenarios asociados a la ciberprotección de las cadenas logísticas, dado que todas ellas sufren un acelerado proceso de despliegue de avanzados sistemas de sensorización y de algoritmos automatizados de procesos de toma de decisión, con el objetivo de mejorar la eficiencia de los servicios prestados, impactando, de forma grave, incluso, en la seguridad física del cliente.

Edificios inteligentes, cámaras frigoríficas conectadas, elaboración automatizada de alimentos, robotización progresiva de los servicios de asistencia y atención, sistemas de vigilancia del establecimiento, ascensores conectados, sistemas de control de presencia

que disparan procesos de calefacción o refrigeración de estancias, sistemas de entretenimiento conectados a servicios de IA... En este sector, como en muchos otros, incluyendo nuestros propios domicilios, el proceso de despliegue de elementos de sensorización y control domótico y logístico es imparable.

Una particularidad del modelo la constituye la ausencia de control sobre los elementos que conforman la red de sensorización y sistemas automatizados de toma de decisión: estamos ante un escenario en el que miles de dispositivos, con capacidad de cómputo, de almacenamiento y de interconexión son desplegados, en cada infraestructura turística, conformando una red de sensorización y de procesos de toma de decisión automatizada con elementos que han sido adquiridos y desplegados con criterios de ahorro económico. Un conjunto de dispositivos que son fabricados al menor coste posible, en zonas geopolíticas diversas y dispersas, donde el control y cumplimiento en materia de ciberseguridad es, cuando menos, difícil de asegurar. Algo parecido a lo que acontece con el desarrollo de algoritmos orientados a los procesos de toma de decisión automatizada donde se intenta minimizar los costes a base de contratar servicios de bajo coste y con un nulo control sobre la ciberseguridad del *software*.

Nada, por otra parte, diferente a lo que ocurre en otros sectores pero que, necesariamente se ha de tener en cuenta cuando intentamos incorporar un cumplimiento exhaustivo en materia de ciberseguridad, al que nos obliga la ley y que es requerido para el buen funcionamiento y la buena reputación del sector en su conjunto sin olvidar el impacto que sobre el negocio causaría un ciberataque exitoso contra el mismo, tanto de índole reputacional como económico, de forma directa.

Este escenario complejo se completa con la conectividad existente con los proveedores logísticos (servicios básicos, alimentos, mantenimiento...) que constituyen un punto de entrada para nue-

vas amenazas y a los que se le debe exigir un cumplimiento de medidas de ciberseguridad que, a menudo, no se encuentra al alcance de pequeños proveedores.

Volvemos, pues, a la cuestión señalada al inicio: ¿Cómo manejamos esta complejidad, estructurada en capas, en esta materia tan técnica y que, además, tiene un nicho de talento accesible muy limitado?

Porque este es otro de los problemas estructurales al modelo: la indisponibilidad de recursos de talento especializado y de buena calidad, para incorporar las medidas mitigadoras de los riesgos y amenazas en materia de ciberseguridad.

En un mundo globalizado y en el sector de la tecnología, los procesos de deslocalización del talento especializado son imparables. Ya no es preciso tomar decisiones vitales, que afecten a las personas expertas y a sus familias, que les obliguen a emigrar y reubicarse en un país concreto para ofrecer sus servicios especializados, sino que éstos pueden prestarse desde cualquier punto del globo que tenga acceso a una red rápida de telecomunicaciones.

¡Por cierto!, un riesgo para el sector, pero también una enorme oportunidad para atraer a una población generadora de actividades de alto valor añadido a nuestro país, con fuerte impacto en el sector turístico. ¿Reflexionamos sobre ello y generamos políticas de atracción sobre este público objetivo?

Pero, volviendo al tema del talento disponible, ¿cómo accedemos al mismo en condiciones óptimas? ¿Cómo lo retenemos, en un sector estratégico para nuestro país? ¿Qué acciones, tanto en materia retributiva como de recompensa podemos desarrollar para que un talento, en principio, tan extraño a un sector que se relaciona con las actividades de bajo valor añadido, considere atractivo desarrollarse profesionalmente en este sector, con necesidades especiales en esta materia?

Tendremos que tomar decisiones inmediatas en este sentido y elaborar políticas públicas que estimulen la formación profesional especializada en materia de ciberseguridad y de inteligencia artificial en el sentido de lo expuesto en el Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información[3] así como en el Real Decreto 279/2021, de 20 de abril, por el que se establece el Curso de Especialización en Inteligencia Artificial y Big Data[4], por supuesto, dotando de recursos suficientes a los centros de Formación Profesional que impartan estas formaciones especializadas de nivel táctico-operativo, tan necesarias para impulsar a cualquier sector productivo, más aún el del turismo. Invertir en ello, sin escatimar medios ni asustarse por cualquier fracaso parcial en el corto plazo, aseguraría la generación de un ecosistema de excelencia que podría posicionar a nuestro país entre los más innovadores de nuestro entorno.

Una vez descrito el escenario y señalados los riesgos, amenazas y oportunidades que, a mi juicio, parecen evidentes, deberíamos glosar y poner en valor algunas iniciativas que, desde el Estado, intentan ofrecer un conjunto de activos de conocimiento relevantes, en materia de ciberseguridad, para el sector turístico.

Así, en noviembre de 2021, el Instituto Nacional de Ciberseguridad (INCIBE) y la Sociedad Mercantil Estatal para la Gestión de la Innovación y las Tecnologías Turísticas (SEGITTUR) publicaron la primera *Guía de ciberseguridad para empresas del sector turístico*[5] en la que se referencian un conjunto de informaciones básicas orientadas a proteger los activos de tratamiento de la información más comunes de un establecimiento turístico tipo.

El sector turístico posee una serie de elementos diferenciadores que generan riesgos específicos que han de tenerse en cuenta a la hora de diseñar y desplegar servicios y sistemas de ciberseguridad y que han sido señalados anteriormente.

La dificultad para establecer un perímetro de seguridad adecuado a las particularidades del sector es más alta de lo que a primera vista parece, sobre todo si tomamos en consideración la renuencia de los decisores estratégicos de los grandes operadores del sector a aceptar la necesidad de la inversión en ciberseguridad como primera línea de defensa del propio negocio y la imposibilidad de asumir el gasto de inversión de los pequeños operadores con recursos propios, siempre limitados y que, a nuestro juicio, debería apoyarse en algún modelo de mutualización de los servicios a través de empresas especializadas que traten a estos pequeños operadores como nodos de una red que comparte necesidades de ciberprotección comunes.

Como conclusiones a este breve análisis de las necesidades de un sector que constituye una de las columnas de nuestro modelo económico, me gustaría reseñar las siguientes:

— La introducción de tecnología en este sector es imparable. Han de promoverse nuevos modelos de negocio que permitan satisfacer las crecientes necesidades de una población objetivo que ya no apuesta sólo por unos precios asequibles, un clima agradable y una atención inmejorable, sino que requiere de servicios de comunicación avanzados y ciberseguros en un entorno laboral en el que la conectividad, continuada o puntualmente necesaria, debe de ser un valor añadido que atraiga nuevo público, de alto poder adquisitivo.

— La ciberseguridad es una inversión del modelo y no un gasto. Debe configurarse como un elemento estructural a cualquier proceso de toma de decisión del negocio. El riesgo inherente a no hacerlo puede impactar, gravemente, en la propia continuidad del negocio.

— Se ha de apostar por modelos mutualizados de aprovisionamiento de servicios cuando no se disponga de recursos suficientes

para desplegar acciones de cumplimiento normativo en esta materia. El talento de buena calidad disponible es escaso y, por lo tanto, caro. Pero pensemos, como decisores en que aún puede resultar más caro sufrir un ciberataque exitoso contra nuestras infraestructuras de servicios.

— La formación de talento táctico-operativo en materias conexas a la ciberseguridad y la inteligencia artificial es, además de necesaria, una inversión de futuro que, para este sector redundará en una mejora en la calidad de los servicios prestados al turista.

E. A. G.

---

[1] Fuente CEOE: https://www.ceoe.es/es/ceoe-news/economia/la-aportacion-del-turismo-al-pib-en-2021-sera-de-77200-millones-la-mitad-que-en#

[2] https://www.destinosinteligentes.es/

[3] BOE núm. 134, de 13 de mayo de 2020.

[4] BOE núm. 111, de 10 de mayo de 2021.

[5] https://www.segittur.es/wp-content/uploads/2021/11/Guia-ciberseguridad-para-empresas-turisticas.pdf