UNIVERSIDAD MIGUEL HERNÁNDEZ DE ELCHE

Facultad de Ciencias Sociales y Jurídicas de Orihuela

Grado en Administración y Dirección de Empresas

LA CIBERSEGURIDAD Y EL TRATAMIENTO DE DATOS PERSONALES EN LAS TRANSACCIONES ONLINE: EL CASO DE BOOKING.COM

Autora: Elena Sánchez Muñoz

Tutor: José Francisco Parra Azor

Orihuela, junio de 2025

Curso académico 2024/2025

ÍNDICE

RESUMEN

Este trabajo analiza la ciberseguridad como un elemento clave para proteger la información y los activos digitales, garantizando la confidencialidad, integridad y disponibilidad de los sistemas. Además de estos principios fundamentales, se abordan aspectos como la autenticación, la autorización, el no repudio y la gestión continua de riesgos. La ciberseguridad moderna se basa en tres pilares interconectados: personas, procesos y tecnología, siendo el factor humano uno de los puntos más vulnerables. En este contexto, la confianza digital se convierte en un factor esencial para la experiencia del usuario en línea, especialmente en sectores como el comercio electrónico y los servicios digitales.

El estudio se centra en el análisis de la plataforma Booking.com y su gestión de la ciberseguridad y el tratamiento de los datos personales de usuarios y colaboradores. Se examinan incidentes de seguridad relevantes y las medidas adoptadas por la empresa, como el uso de cifrado, autenticación multifactor y auditorías internas, así como su grado de cumplimiento con el Reglamento General de Protección de Datos (RGPD). Aunque Booking.com ha implementado avances significativos, se identifican debilidades, especialmente en la formación del personal de los hoteles afiliados y en la seguridad fuera de su infraestructura principal.

Palabras clave: Booking.com, Ciberseguridad, Protección de datos personales, Reglamento General de Protección de Datos (RGPD),

ABSTRACT

This paper analyzes cybersecurity as a key component for protecting digital assets and information, ensuring the confidentiality, integrity, and availability of systems. Beyond these core principles, it addresses additional aspects such as authentication, authorization, non-repudiation, and continuous risk management. Modern cybersecurity relies on the interconnection of three essential pillars: people, processes, and technology, among which the human factor remains the most vulnerable. In this context, digital trust has become fundamental to the online user experience, particularly in digital service and e-commerce platforms.

The study focuses on Booking.com and its approach to cybersecurity and the handling of personal data of users and partners. Several security incidents and the company's responses are examined, including the implementation of encryption, multi-factor authentication, and internal audits, along with compliance with the General Data Protection Regulation (GDPR). While Booking.com has made significant progress, weaknesses remain, especially regarding staff training in partner hotels and the security of systems outside its core infrastructure.

Keywords: Booking.com, Cybersecurity, Personal Data Protection, General Data Protection Regulation (GDPR)

1. Introducción

La digitalización representa uno de los procesos más transformadores del siglo XXI, al trascender la mera incorporación de nuevas tecnologías para implicar una reconfiguración profunda de las dinámicas sociales, culturales y empresariales. En el ámbito corporativo, este fenómeno ha permitido optimizar procesos, mejorar la relación con los clientes y adaptarse con mayor agilidad a un mercado global en constante evolución. Además, ha dado lugar a modelos de negocio innovadores y a una experiencia del cliente más personalizada y eficiente. Desde la Revolución Industrial hasta nuestros días, la adopción tecnológica ha sido clave para aumentar la productividad, pero es en la actualidad cuando la digitalización se ha consolidado como una estrategia esencial para la competitividad. En este contexto, la Unión Europea ha reconocido la relevancia de la transformación digital, promoviendo inversiones en infraestructura, legislación y educación con el fin de cerrar la brecha digital y reforzar la posición estratégica de sus economías. Esta transformación no solo tiene implicaciones técnicas, sino también sociales, económicas y jurídicas, especialmente en lo relativo al uso y protección de los datos personales en entornos digitales.

Uno de los sectores más impactados por esta evolución es el del comercio digital, donde plataformas como Booking.com desempeñan un papel central. Su funcionamiento depende de la gestión eficaz de grandes volúmenes de datos y de la confianza que los usuarios depositan en su seguridad. En este contexto, la ciberseguridad se convierte en un elemento fundamental, no solo para la protección técnica de los sistemas, sino también para asegurar el cumplimiento normativo y preservar la reputación de la empresa.

El presente Trabajo Fin de Grado tiene como objetivo general analizar en profundidad las políticas y prácticas de ciberseguridad, así como el tratamiento de datos personales que lleva a cabo la plataforma Booking.com, evaluando su adecuación al marco normativo vigente y su efectividad frente a las amenazas actuales.

De forma específica, se plantea:

- Describir los problemas de ciberseguridad que ha presentado Booking.com a lo largo de su actividad empresarial.
- Analizar si el tratamiento de datos personales y las medidas de protección adoptadas por la plataforma se ajustan al marco legal actual.

- Proponer una serie de indicadores y recomendaciones que permitan a Booking.com reforzar su cumplimiento normativo y garantizar un manejo seguro de la información de clientes y colaboradores.

1.1. La ciberseguridad y el comportamiento del consumidor online

La ciberseguridad, o seguridad digital, es la disciplina esencial que protege la información, los dispositivos y los activos digitales de individuos y organizaciones. Su alcance va mucho más allá de la informática tradicional, abarcando desde datos personales y financieros hasta redes, entornos en la nube, dispositivos móviles, etc. (Liu et al., 2022). Los objetivos principales de la ciberseguridad son cuidar la confidencialidad, la integridad y la disponibilidad de los sistemas y la información. Esto significa proteger datos delicados con cifrado y reglas de acceso, además de prevenir y responder bien a los ciberataques. Se busca que los sistemas y redes sigan funcionando, aunque haya incidentes, asegurando que la información sea exacta, completa y que solo puedan verla los usuarios autorizados. Además, la ciberseguridad es clave para reducir riesgos, evitar grandes pérdidas y conseguir que todo vuelva a la normalidad rápidamente después de un problema, siempre cumpliendo con la ley (Liu et al., 2022).

Más allá de la clásica tríada de Confidencialidad, Integridad y Disponibilidad (CIA), la ciberseguridad actual añade principios muy importantes para una defensa sólida. En los últimos años se han incorporados los conceptos de la autenticación (para saber quién es quién), la autorización (para ver si alguien tiene permiso para hacer algo), el no repudio (para que nadie pueda negar lo que ha hecho) y la evaluación constante de riesgos (Borky y Bradley, 2018). Estos puntos son fundamentales para generar confianza y asegurar que haya responsabilidades en el complejo mundo digital de hoy. No basta con proteger los datos; es igual de importante saber quién entra, qué hace y si tenía permiso para ello. La ciberseguridad se apoya en tres pilares que dependen uno del otro: las personas, los procesos y la tecnología. La tecnología proporciona las herramientas y los sistemas para protegernos, como los firewalls o el cifrado. Los procesos nos dicen cómo aplicar y gestionar esas defensas, incluyendo qué hacer si hay un incidente. Pero el pilar más impredecible es el de las personas, porque un simple despiste o la falta de información pueden abrir la puerta a problemas de seguridad. Los fallos de seguridad a menudo aprovechan el punto más débil, que muchas veces es el factor humano a través de técnicas como la ingeniería social. Por eso, para tener una ciberseguridad realmente fuerte, hay

que invertir de forma continua y coordinar muy bien estos tres pilares, entendiendo que trabajan juntos para una defensa completa y resistente (Borky y Bradley, 2018).

1.2. Importancia de la ciberseguridad en la experiencia del usuario online

La ciberseguridad es clave para la experiencia del usuario en línea, ya que construye y mantiene la confianza digital. Confiar en estos sistemas es vital para proteger a las empresas de ataques complejos y para que los usuarios se sientan seguros al interactuar en el entorno digital. No obstante, la sensación constante de vulnerabilidad, por filtraciones de datos, ataques de *ransomware* y desinformación, desgasta esa confianza. Además, la poca transparencia de las organizaciones sobre cómo manejan los datos aumenta el escepticismo y, cuando los clientes se sienten seguros al interactuar en línea, están más dispuestos a compartir información, comprar y mantener su relación con una empresa (Saeed et al., 2023). Hoy en día, la ciberseguridad ha dejado de ser un simple coste o un requisito técnico para convertirse en una estrategia. En el entorno digital una buena ciberseguridad se traduce directamente en más confianza digital. Esta confianza, a su vez, se vuelve un diferenciador clave para las empresas, atrayendo y fidelizando a clientes que valoran la seguridad y privacidad de sus datos. En contraste, un fallo de seguridad puede dañar seriamente esta confianza, llevando a la pérdida de clientes y a un impacto negativo en la reputación, que afecta directamente a los resultados económicos de la empresa.

Uno de los objetivos principales de la ciberseguridad es proteger los datos personales de los usuarios que hacen compras *online*. La privacidad en línea se refiere a la cantidad de información sobre un individuo disponible en Internet y es fundamental que las personas mantengan el control sobre sus datos personales y quién accede a ellos. Esto implica necesariamente un tratamiento transparente, limitando su recopilación y su uso, asegurando así una gestión responsable. Para ello, se aconsejan prácticas como actualizar el software a menudo, usar contraseñas seguras y únicas y leer con atención las políticas de privacidad y ser moderado al compartir en redes, entre otras.

La seguridad en Internet es una responsabilidad compartida. Aunque las organizaciones tienen una responsabilidad importante en la seguridad y privacidad de los datos, los usuarios también juegan un papel activo. Formar a los usuarios con conocimientos y herramientas, como el uso de contraseñas robustas o el reconocimiento del *phishing*, es fundamental. En resumen, podemos decir que una ciberseguridad deficiente puede traer

una mala reputación para la empresa, poniendo en riesgo su continuidad mientras que integrar la seguridad con la experiencia del cliente puede diferenciar a las empresas, permitiendo ofrecer servicios personalizados sin comprometer la privacidad. Por lo tanto, una ciberseguridad robusta se convierte en un atributo de marca, generando lealtad y crecimiento (Saeed et al., 2023).

1.2.1. Brechas en la ciberseguridad.

Las brechas de seguridad representan una de las mayores amenazas en el entorno digital y pueden causar grandes problemas tanto en organizaciones como a los usuarios (Nawaz et al., 2023). Entre los más comunes se encuentra el *malware*, un software malicioso diseñado para interrumpir, dañar o acceder sin permiso a sistemas informáticos. Este término incluye, virus, gusanos, troyanos (como RATs y *droppers*), *ransomware* (que cifra sistemas y exige rescate), *spyware* (que recopila información sensible de forma oculta) y *rootkits* (que otorgan acceso a nivel de administrador). Otro ataque frecuente es el *phishing* y el *spear phishing*, que consisten en el envío de correos electrónicos o mensajes fraudulentos que suplantan a entidades para robar información privada o distribuir *malware*. El *spear phishing*, en particular, se distingue por ser altamente dirigido y personalizado. Los ataques de Denegación de Servicio (*DoS*, por sus siglas en inglés) y Denegación de Servicio Distribuida (*DDoS*) buscan saturar un sistema con tráfico para hacerlo inaccesible a usuarios legítimos.

La ingeniería social manipula a individuos para que revelen información confidencial o realicen acciones indebidas, usando tácticas como el *baiting*, el *shoulder surfing*, el *dumpster diving*, el spam y los fraudes online. Otros ataques habituales incluyen la inyección SQL, el *man-in-the-middle*, las redes Wi-Fi trampa y la suplantación. A pesar de la complejidad de las defensas tecnológicas como los antivirus, la experiencia nos muestra de forma constante que la vulnerabilidad humana es la debilidad más explotada.

En la **Tabla 1** se puede encontrar un resumen de estas amenazas, así como las consecuencias más usuales para empresas y usuarios.

Tabla 1.- Amenazas más frecuentes y sus consecuencias.

Tipo de Ciberataque	Descripción Breve	Consecuencias para Empresas	Consecuencias para usuarios
Malware (Ransomware, Spyware, Troyanos)	Software malicioso que interrumpe, daña, roba datos o secuestra sistemas.	Pérdidas financieras, interrupción operativa, pérdida de datos, daño reputacional.	Robo de información personal/financiera, secuestro de dispositivos, pérdidas económicas.
Phishing / Spear Phishing	Engaño (usualmente por email) para obtener información confidencial o instalar malware.	Robo de credenciales/datos sensibles, filtraciones de datos, propagación de malware.	Robo de identidad, pérdidas financieras, acceso no autorizado a cuentas.
Denegación de Servicio (DoS/DDoS)	Saturación de sistemas con tráfico para impedir el acceso legítimo.	Interrupción de servicios, pérdida de ingresos, daño a la reputación.	Imposibilidad de acceder a servicios en línea, frustración.
Ingeniería Social (Baiting, Shoulder Surfing, Spam, Fraudes Online)	Manipulación psicológica para que las víctimas revelen información o realicen acciones.	Filtración de datos, fraude, acceso no autorizado a sistemas.	Robo de identidad, pérdidas económicas, extorsión, daño al honor.
Ataques a Contraseñas (Fuerza Bruta, Diccionario)	Intentos sistemáticos de adivinar credenciales de acceso.	Acceso no autorizado a sistemas, robo de datos, compromiso de cuentas.	Robo de identidad, acceso a cuentas personales, pérdidas financieras.

*Fuente: Elaboración propia.

1.3. Regulación y protección de la información digital: políticas de ciberseguridad y tratamiento de datos personales en España y el sector hotelero.

1.3.1 Políticas de ciberseguridad en España.

España ha desarrollado un marco robusto y en constante evolución en materia de ciberseguridad. Por ejemplo, el Real Decreto-ley 12/2018 transpuso la Directiva NIS europea, estableciendo requisitos de seguridad y notificación de incidentes para infraestructuras críticas y servicios esenciales como energía, transporte, banca y salud, así

como para proveedores de servicios digitales. En 2018, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) consiguió adaptar la legislación nacional al Reglamento General de Protección de Datos (RGPD) de la UE, garantizando la protección de los datos personales y los derechos digitales de los ciudadanos. Además, existe el llamado Esquema Nacional de Seguridad (ENS), que fue establecido en 2010 y actualizado en 2025, y que consiste en un marco normativo que define principios y requisitos de ciberseguridad para los sistemas de información de la Administración Pública y sus proveedores. Existen muchas otras leyes, como la Ley de Protección de Infraestructuras Críticas (Ley 8/2011), que se centra en reforzar la seguridad y resiliencia de los activos esenciales para la economía y la seguridad nacional, o el Real Decreto 43/2021, que amplía las obligaciones de seguridad de la Directiva NIS en redes y sistemas de comunicación electrónica. La Ley General de Telecomunicaciones (Ley 11/2022) fortalece la seguridad y resiliencia de las infraestructuras de telecomunicaciones, exigiendo a los operadores la adopción de medidas de seguridad y la notificación de incidentes relevantes. Cabe destacar también la Ley 6/2020, que regula aspectos de los servicios electrónicos de confianza. Todas estas leyes y normativas buscan asegurar que las defensas del país sigan siendo pertinentes y efectivas, fomentando así la confianza digital y la innovación (Del-Real y Díaz-Fernández, 2022).

La influencia de la normativa europea es fundamental en la configuración de las políticas de ciberseguridad en España. La Directiva NIS (2016/1148) estableció un alto nivel común de seguridad en las redes y sistemas de información en la UE. Posteriormente, la Directiva NIS2 (UE 2022/2555) actualizó y amplió el alcance de NIS a más sectores, como energía, transporte, salud y servicios digitales, exigiendo a las entidades afectadas implementar medidas de seguridad y notificar incidentes importantes en un plazo de 24 horas. España adaptó finalmente su legislación nacional a NIS2 mediante el Real Decreto-ley 12/2022. Además, el Reglamento General de Protección de Datos (RGPD) (UE 2016/679) es la pieza clave de la protección de datos en la UE, con su transposición en España a través de la LOPDGDD. Este reglamento impone normas estrictas para el tratamiento de datos personales, garantizando la privacidad y estableciendo multas por incumplimiento (Del-Real y Díaz-Fernández, 2022).

1.3.2. Políticas y tratamiento de datos personales en el sector hotelero

El sector hotelero, incluyendo plataformas de intermediación como Booking, se enfrenta a un desafío de ciberseguridad debido al gran volumen y la sensibilidad de los datos que

maneja. Los hoteles recopilan una cantidad enorme de información personal y financiera de sus huéspedes, como nombres, direcciones, datos de tarjetas de crédito e incluso información de salud. La industria hotelera es un objetivo muy atractivo para los ciberdelincuentes no solo por el volumen, sino por el tipo de información que maneja, ya que los datos financieros y de salud son altamente sensibles y muy valiosos en los mercados ilegales. Este perfil de datos, junto a la alta frecuencia de transacciones online de las operaciones hoteleras, crea un entorno de alto riesgo para empresas y usuarios (Jaione Vertiz Aguirre, 2023)

Los hoteles están obligados a justificar legalmente cualquier tratamiento de datos personales, ya sea por la relación contractual con el cliente (como en el caso de las reservas), por exigencias legales (como el registro obligatorio de viajeros), porque el huésped haya dado su consentimiento expreso (para campañas de marketing) o por intereses legítimos del establecimiento como la mejora de sus servicios. Es fundamental que cada hotel cuente con una política de privacidad comprensible y fácil de consultar, donde se especifique qué información se recaba, con qué finalidad, durante cuánto tiempo se conserva y qué derechos asisten al cliente respecto a sus datos. Paralelamente, deben establecerse protocolos de seguridad efectivos que incluyan sistemas de encriptación, controles de acceso, capacitación periódica del personal y auditorías internas para prevenir vulnerabilidades. Las consecuencias por incumplir estas normas pueden ser severas. En casos graves, como procesar datos sin base legal o no atender las solicitudes de los titulares, las multas pueden alcanzar hasta 20 millones de euros o el 4% del volumen de negocio anual. Hay infracciones concretas que suelen pasar desapercibidas, como guardar copias del DNI sin justificación válida o conservar información más allá del plazo estrictamente necesario (Jaione Vertiz Aguirre, 2023).

En cuanto al Real Decreto 933/2021 sobre Registro de Viajeros, esta normativa es de aplicación obligatoria para todos los alojamientos turísticos y plataformas digitales de intermediación y establece la recogida sistemática de información detallada: desde los datos personales del viajero (nombre completo, documento de identidad, nacionalidad, datos de contacto) hasta los detalles menores de la estancia (fechas, características del alojamiento, detalles del pago). Toda esta información debe remitirse a las autoridades competentes a través de la plataforma SES.HOSPEDAJES en un plazo máximo de 24 horas. El incumplimiento de estos requisitos puede acarrear sanciones económicas que oscilan entre los 601 y los 30.000 euros, además de permitir a los establecimientos poder

denegar la entrada a aquellos huéspedes que se nieguen a facilitar la información requerida (SES Hospedajes, 2025).

En cuanto a las transacciones online, uno de los métodos más utilizados por las empresas hoteleras es el uso de pasarelas de pago seguras, como Stripe, PayPal o Redsys, que cifran la información financiera y evitan que los datos sensibles (como números de tarjeta) queden almacenados en los sistemas del hotel. Además, muchos hoteles integran TPVs virtuales (Terminales Punto de Venta) en sus webs y sistemas de reserva, lo que permite aceptar pagos online sin necesidad de intervención manual. Para prevenir fraudes, se emplean herramientas de análisis de riesgo y autenticación reforzada, como la verificación 3D Secure, que añade un paso adicional de confirmación, como un código

2. Análisis de la ciberseguridad y protección de datos en Booking.com

2.1. Evolución de la Ciberseguridad y Protección de Datos en Booking.com

En el contexto del turismo digital contemporáneo, las plataformas de reserva en línea, como Booking.com, se han consolidado como intermediarios clave al facilitar la conexión entre proveedores de alojamiento y clientes a escala global. Esta función implica necesariamente la recopilación y tratamiento de una gran cantidad de datos personales, que incluyen información de identificación, detalles financieros y preferencias de servicio. Como consecuencia, surge una elevada concentración de información sensible, lo que incrementa las vulnerabilidades en materia de ciberseguridad.

Una posible brecha de seguridad no solo conlleva la exposición de datos confidenciales de los usuarios, sino que también puede acarrear graves consecuencias para la empresa, entre ellas daños reputacionales, perjuicios económicos significativos y posibles sanciones por el incumplimiento de normativas en materia de protección de datos personales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Ante este panorama, Booking.com afirma en sus fuentes oficiales su compromiso con el cumplimiento de la legislación vigente en materia de privacidad incluyendo el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. La compañía implementa diversas medidas técnicas y organizativas para proteger la confidencialidad, integridad y disponibilidad de los datos personales (Booking.com, 2025). Además, al operar en un mercado globalizado Booking.com realiza transferencias internacionales de datos a países fuera del Espacio Económico Europeo (EEE). En estos casos, la empresa aplica medidas de seguridad adicionales, como cláusulas contractuales aprobadas por la Comisión Europea, con el objetivo de asegurar garantizar la protección de los datos personales (Booking.com, n.d.).

2.2. Brechas en la ciberseguridad de Booking.com

A lo largo de los últimos años Booking.com ha enfrentado numerosos incidentes de seguridad que han evolucionado desde vulnerabilidades técnicas puntuales hasta campañas de phishing altamente sofisticadas. Estas brechas han afectado tanto a clientes como a socios comerciales, revelando la persistencia de fallos en la protección de datos y la coordinación entre los actores implicados en la plataforma. Consiste principalmente en accesos no autorizados a cuentas de hoteles y usuarios. La usurpación de canales de

comunicación interna de la plataforma (como el chat web) para estafar a clientes ha sido denunciada en varias ocasiones. También han ocurrido ataques de phishing y estafas dirigidas a empleados de hoteles *(*"ClickFix phishing scam," 2023).

En los últimos meses se ha reportado un incremento en ataques de phishing dirigidos a clientes de Booking.com, según el artículo "Fake Booking.com messages" (2025). Los ciberdelincuentes se hacen pasar por hoteles o la propia plataforma, enviando correos o mensajes fraudulentos para robar datos de pago. Según Bleeping Computer (2023), algunos usuarios recibieron mensajes solicitando el pago anticipado mediante enlaces falsos, lo que llevó a pérdidas económicas. Booking.com ha admitido que algunos socios hoteleros también han sido víctimas de brechas de credenciales, lo que permite a los atacantes acceder a los sistemas de reservas (Europa Press, 2025).

Investigadores de ciberseguridad han identificado posibles vulnerabilidades en las APIs de Booking.com que podrían permitir el acceso no autorizado a información de reservas. En 2024, se notificó un caso donde datos de clientes (nombres, fechas de reserva y detalles de alojamiento) fueron filtrados debido a una mala configuración en un servidor proporcionado por un proveedor externo (Microsoft, 2025). También han sido víctima de ataques B2B (Business To Business) dirigidos a socios comerciales (hoteles y alojamientos). Los atacantes comprometen las cuentas de los administradores de estos establecimientos para modificar detalles de pago y desviar fondos (Europa Press, 2025).

A principios de 2016 se reportó el primer ciberataque a Booking.com. En esta ocasión el ataque fue descubierto casi por accidente cuando se identificó un acceso no autorizado que utilizaba un servidor con seguridad deficiente, a través del cual se lograba extraer información de miles de reservas ubicadas principalmente en países del Medio Oriente (Arabia Saudí, Qatar, Emiratos Árabes Unidos). El ataque fue realizado un hacker estadounidense, identificado internamente como “Andrew”, con estrechos vínculos a una empresa que trabajaba para agencias de inteligencia de EE. UU. Booking.com movilizó a cuatro especialistas de seguridad que trabajaron durante aproximadamente dos meses para determinar el origen del ataque y atribuirlo. Colaboraron incluso con investigadores privados vinculados a EE. UU., además de solicitar asistencia al servicio de inteligencia neerlandés AIVD. Los datos sustraídos incluían nombre e itinerario (fechas, destino, hotel) de miles de reservas en Oriente Medio Según Booking.com no hubo acceso a datos financieros sensibles (ni tarjetas de crédito ni contraseñas), pero académicos y expertos señalaron que incluso la información de itinerarios personales puede tener efectos graves,

como inclusión en listas de control (por ejemplo, “no-fly” o vigilancia diplomática) (Kaaij y Dohmen, 2021).

En 2018 se reportó otra brecha de ciberseguridad. En diciembre de dicho año, varios delincuentes obtuvieron acceso no autorizado a las cuentas de 40 hoteles en los Emiratos Árabes Unidos, lo que permitió el acceso a los datos personales de más de 4.000 clientes, incluyendo información de tarjetas de crédito de 283 personas. Booking.com no informó a la autoridad de protección de datos de los Países Bajos hasta 22 días después del incidente, lo que resultó en una multa de 475.000 euros por parte de dicha autoridad (Cimpanu, 2021). Fueron un total de 4 109 clientes afectados y se accedió a datos personales de más de cuatro mil usuarios, incluyendo nombre, dirección, teléfono e información de la reserva (fechas de estancia, destino, hotel, etc.).

En 2022 Booking sufrió un nuevo ciberataque. Este ataque fue detectado por investigadores de Salt Labs y detectaron varios errores en cómo Booking.com manejaba su inicio de sesión mediante OAuth con Facebook. La investigación mostró que los atacantes eran capaces de realizar un secuestro de cuenta completo (Account Takeover) sin necesidad de robar la contraseña del usuario usando URLs maliciosas especialmente manipuladas (Salt Security, 2023). En esta ocasión, la brecha de ciberseguridad afectó a millones de usuarios.

En 2023, se produjo una campaña de phishing a gran escala dirigida a clientes de Booking.com a través de hoteles colaboradores. Los ciberdelincuentes accedieron a cuentas de gestión de los alojamientos tras infectar los ordenadores del personal con programas que robaban contraseñas. Con el control de esas cuentas, enviaban mensajes desde la propia plataforma de Booking.com pidiendo a los usuarios que confirmasen sus datos de pago mediante enlaces falsos que imitaban la web oficial. Muchos viajeros cayeron en la trampa, creyendo que se trataba de mensajes auténticos. El ataque afectó a cientos de establecimientos en todo el mundo (BleepingComputer, 2023; Perception Point, 2023). De nuevo en 2023, se detectó una nueva oleada de estafas relacionadas con Booking.com. Los atacantes accedieron al correo electrónico de varios hoteles y, desde ahí, enviaron mensajes que parecían oficiales (incluso desde direcciones como “noreply@Booking.com.com”) pidiendo a los clientes que confirmasen sus datos de pago a través de enlaces fraudulentos. Aunque Booking.com negó que su sistema hubiese sido vulnerado directamente, reconoció que los ciberdelincuentes utilizaron cuentas de hoteles reales para llevar a cabo el engaño. Muchos usuarios sufrieron cargos no autorizados y se

generó una gran confusión. En respuesta, la plataforma reforzó sus controles de seguridad y lanzó advertencias tanto a los viajeros como a los establecimientos. Según las autoridades australianas, este tipo de estafas aumentó un 580 % durante el año, con pérdidas que ascendieron a cientos de miles de dólares (Knaus, 2024;).

En 2024 se intensificaron los fraudes relacionados con Booking.com, especialmente en Hungría y Australia. En Hungría, entre noviembre de 2024 y enero de 2025, unos 112 usuarios denunciaron estafas por phishing: los atacantes suplantaban correos de hoteles afiliados, clonaban la web y robaron cerca de 440.000 € en solo tres meses. Simultáneamente, en Australia, según la ACCC, en 2023 hubo 363 denuncias ligadas a Booking.com, con pérdidas de más de 337 000 dólares (un incremento del 580 % respecto al año anterior) gracias a emails cada vez más convincentes generados por IA. Booking.com reconoció que no se había vulnerado su infraestructura principal, sino que muchos casos venían de cuentas asociadas a hoteles. En respuesta, la empresa reforzó sus sistemas y alertó a usuarios y plataformas sobre la necesidad de extremar precauciones (Knaus, 2024). Incluso en 2025 existen incidencias. En marzo de este año varios usuarios informaron en Reddit que se siguen filtrando mensajes de phishing dentro del sistema de mensajería de Booking.com, enviados desde propiedades afectadas. Los enlaces parecen conducir a réplicas casi exactas del portal oficial, pero con dominios falsos (“Phishing attacks,” n.d.).

Es importante señalar que los problemas de ciberseguridad en Booking.com han pasado de ser vulnerabilidades aisladas a convertirse en campañas de phishing cada vez más elaboradas, perjudicando tanto a clientes como a los propios hoteles colaboradores. Pese a las mejoras implementadas por la plataforma, como la verificación en dos pasos o sistemas de monitorización avanzada, el hecho de que estos ataques sigan repitiéndose pone de manifiesto dos carencias clave: la falta de coordinación con los establecimientos afiliados y la escasa formación de muchos usuarios. Los casos registrados en 2024 y 2025 confirman que el principal riesgo sigue estando en el comportamiento de las personas, ya sea por fallos en la gestión de los alojamientos o por la facilidad con la que los viajeros caen en trampas bien diseñadas. En este contexto, resulta esencial que futuros estudios profundicen en estrategias integrales que combinen inteligencia artificial, protocolos de actuación coordinados entre los actores del sector y campañas educativas dirigidas tanto a empleados como a viajeros, con el fin de mitigar los riesgos de ciberataques en plataformas de intermediación turística como Booking.com

2.3. Evolución de Booking.com en la protección de datos

Desde su fundación en 1996 en Ámsterdam, Booking.com ha transitado un largo camino en la manera en que gestiona y protege los datos personales de sus usuarios. Esta evolución ha estado marcada por el crecimiento acelerado de la economía digital, el aumento exponencial en la cantidad de información procesada y, sobre todo, por el fortalecimiento de los marcos normativos, como el Reglamento General de Protección de Datos (RGPD). En sus inicios, la plataforma operaba en un entorno donde la protección de datos era todavía una preocupación secundaria, tanto para empresas como para usuarios. Las primeras políticas de privacidad de Booking.com eran escuetas, redactadas en un lenguaje técnico poco accesible, y orientadas principalmente a permitir un funcionamiento eficiente del sistema de reservas (Acquisti et al., 2015). Durante la primera década de su actividad, la atención se centraba en garantizar la funcionalidad y rapidez del servicio, recolectando únicamente datos básicos como el nombre, correo electrónico, preferencias de alojamiento y detalles de pago. No obstante, la evolución del comercio electrónico y la proliferación de tecnologías móviles y de seguimiento digital incrementaron significativamente tanto la cantidad como la sensibilidad de los datos recabados. Esto hizo evidente la necesidad de una regulación más estricta y de una adaptación organizativa en empresas como Booking.com, que pasaron de ser plataformas de servicios a verdaderos centros de tratamiento masivo de datos personales (Schwartz & Solove, 2020).

Un punto de inflexión fundamental fue la entrada en vigor del RGPD en mayo de 2018. Esta normativa, pionera en establecer un estándar europeo con proyección global, exigió a las empresas una serie de obligaciones precisas en materia de protección de datos, incluyendo el consentimiento explícito, el derecho al acceso, rectificación y supresión, así como la obligación de implementar medidas técnicas y organizativas adecuadas para prevenir el acceso no autorizado a la información personal. En cumplimiento con estas exigencias, Booking.com revisó de manera integral sus políticas de privacidad. Entre los cambios más significativos se encuentra la adopción de un lenguaje más claro y comprensible para el usuario, la inclusión de apartados detallados sobre los fines del tratamiento de datos, la duración del almacenamiento y los mecanismos de protección, y la habilitación de herramientas para que los propios usuarios pudieran gestionar su información mediante paneles de control personalizados (Booking.com, 2018).

Asimismo, la empresa incorporó los principios de *privacy by design* y *privacy by default*, integrando la protección de datos desde la fase de diseño de sus productos digitales. Esta estrategia ha supuesto también una inversión significativa en sistemas de cifrado, auditorías internas periódicas y protocolos de respuesta ante incidentes de seguridad. Sin embargo, estos esfuerzos no han estado exentos de dificultades. En 2021, la Autoridad de Protección de Datos de los Países Bajos (Autoriteit Persoonsgegevens) impuso a Booking.com una multa de 475.000 euros por no notificar dentro del plazo legal una brecha de seguridad ocurrida en 2018, que comprometió los datos de aproximadamente 4.000 usuarios, incluyendo información sobre tarjetas de crédito (European Data Protection Board, 2020). Este caso reveló ciertas debilidades en los protocolos internos de la empresa para la gestión de incidentes y subrayó la importancia del cumplimiento no solo formal, sino también operativo del RGPD.

Por otro lado, la evolución tecnológica ha traído consigo nuevos desafíos. La integración de funciones avanzadas en las aplicaciones móviles de Booking.com ha permitido acceder a datos como la geolocalización o el comportamiento de navegación, utilizados para ofrecer recomendaciones personalizadas. Si bien estas funcionalidades mejoran la experiencia del usuario, también implican un tratamiento más complejo y sensible de la información personal. A ello se suma la creciente utilización del Big Data para analizar patrones de consumo, optimizar precios y segmentar audiencias. Todo ello requiere compartir ciertos datos con terceros asociados, bajo estrictas condiciones contractuales y legales para garantizar la confidencialidad y la integridad de la información. En respuesta a estas exigencias, Booking.com ha reforzado su estructura organizativa, incluyendo la figura del Delegado de Protección de Datos (DPO), programas de formación continua para empleados y mecanismos para recibir y gestionar reclamaciones de usuarios. La empresa también ha mejorado la transparencia sobre el uso de cookies y tecnologías de rastreo, permitiendo a los usuarios aceptar, rechazar o personalizar su uso de manera sencilla. Actualmente, la compañía no solo cumple con el RGPD, sino que ha extendido sus políticas para adaptarse a normativas extraterritoriales como la Ley de Privacidad del Consumidor de California (CCPA) y otras leyes locales en mercados estratégicos. Este enfoque global responde a la necesidad de generar confianza entre sus usuarios y consolidar su posición en un entorno digital marcado por la creciente sensibilidad social respecto a la privacidad. En este contexto, Booking.com ha manifestado su intención de avanzar hacia modelos de minimización y anonimización de datos, y de explorar

tecnologías como la inteligencia artificial siempre dentro de un marco ético y conforme a derecho.

La trayectoria de Booking.com en materia de protección de datos refleja el tránsito general del sector digital: desde un enfoque meramente funcional y comercial hacia un modelo más robusto, centrado en el respeto a los derechos fundamentales de los usuarios. La empresa parece percibir que la privacidad no es solo un requisito legal, sino un componente esencial para la sostenibilidad y legitimidad de sus operaciones en el largo plazo.

2.4. Indicadores de buenas prácticas y herramientas aplicadas por Booking.com en materia de ciberseguridad y protección de datos personales

2.4.1. Estrategias de ciberseguridad y recursos implementados por Booking.com

A partir del análisis de las brechas de ciberseguridad y del tratamiento de datos personales en Booking.com, se proponen a continuación una serie de indicadores de buenas prácticas y herramientas tecnológicas, organizativas y legales orientadas a mejorar la seguridad y la gestión de datos personales (Pascoe et al., 2024). Estos indicadores están agrupados en función de los dos ejes de análisis:

Uno de los primeros estándares que toda empresa digital debería cumplir es la implementación universal de la autenticación multifactor (MFA), especialmente en las cuentas administrativas y de socios hoteleros, que suelen ser los puntos más atacados. Esta medida permite reducir drásticamente los riesgos asociados a accesos no autorizados. Sin embargo, a pesar de las mejoras técnicas aplicadas por Booking.com en los últimos años, la reiteración de incidentes relacionados con accesos indebidos a cuentas de hoteles demuestra que la MFA no se aplica de forma obligatoria ni generalizada, al menos en el entorno de los socios. Por tanto, si bien la plataforma puede haber avanzado en entornos internos, no puede afirmarse que cumpla plenamente con este indicador.

Otro parámetro fundamental es el tiempo medio de respuesta ante incidentes de ciberseguridad. Un plazo inferior a 24 horas es deseable para contener amenazas antes de que generen daños considerables. Booking.com, sin embargo, ha demostrado carencias importantes en este aspecto. En el incidente de 2018, la empresa tardó 22 días en notificar a las autoridades sobre una filtración que afectó a más de 4.000 clientes. Más recientemente, campañas de phishing realizadas a través de su propio sistema de

mensajería se mantuvieron activas durante días sin ser detectadas, lo que pone en evidencia una capacidad de respuesta aún insuficiente en ciertos casos. A pesar de la inversión en tecnologías de monitoreo, no se ha logrado consolidar un tiempo de reacción ágil y constante que permita cumplir este estándar de manera sistemática.

El porcentaje de dispositivos gestionados con soluciones de protección, como antivirus y herramientas EDR (detección y respuesta en endpoints), es otro indicador de referencia. El objetivo ideal es que al menos el 95 % de los equipos estén protegidos con software actualizado. Aunque no se dispone de datos públicos específicos sobre la infraestructura técnica de Booking.com, los incidentes recurrentes que parten desde los sistemas informáticos de los hoteles sugieren que no existe una política uniforme o una supervisión efectiva de los dispositivos que forman parte de su red de socios. Es posible que en su sede central y áreas técnicas este nivel de protección sea alto, pero en el contexto descentralizado de sus colaboradores, especialmente hoteles pequeños o medianos, el cumplimiento parece ser desigual, lo que impide alcanzar el estándar del 95 %. En paralelo, la formación en ciberseguridad de los empleados y socios también constituye un aspecto crítico (Mahboub y El-Kourdi, 2024). La tasa de éxito en simulaciones de phishing debería alcanzar, como mínimo, el 85 % para considerarse adecuada. Sin embargo, los numerosos casos documentados entre 2023 y 2025 evidencian una falta de preparación generalizada. Muchos de los ataques han tenido éxito precisamente porque los empleados de los alojamientos no supieron identificar correos o enlaces fraudulentos, lo que facilitó el acceso de los atacantes al sistema de mensajería interno. Estas vulnerabilidades humanas, reiteradas a lo largo del tiempo, indican que las campañas de formación no han sido suficientes o bien no se han dirigido correctamente a los eslabones más frágiles de la cadena: los hoteles colaboradores.

Asimismo, las auditorías de ciberseguridad externas representan una herramienta clave para garantizar la objetividad en la evaluación de los sistemas. Se recomienda realizar al menos una auditoría independiente al año. Booking.com, como multinacional que maneja datos personales en el marco del RGPD y otras normativas globales, presumiblemente realiza este tipo de auditorías. Sin embargo, los errores detectados en el uso de sistemas como OAuth o en la configuración de servidores de terceros sugieren que algunas evaluaciones no han sido lo suficientemente exhaustivas como para anticiparse a riesgos conocidos. Es decir, si bien podría afirmarse que existe un cumplimiento básico en cuanto

a la realización de auditorías, su profundidad o alcance parecen requerir una revisión más exigente.

Por último, el cumplimiento con marcos normativos reconocidos, como el Esquema Nacional de Seguridad (ENS) en España o la certificación ISO/IEC 27001 a nivel internacional, aporta un nivel adicional de garantía. Booking.com ha demostrado compromiso con normativas como el Reglamento General de Protección de Datos (RGPD), adoptando medidas como la privacidad desde el diseño, la gestión del consentimiento, y la protección de datos en tránsito y en reposo (ENISA, 2025). No obstante, no hay constancia pública de que la empresa esté certificada bajo ISO/IEC 27001 ni de que haya adoptado el ENS, que, aunque no obligatorio para empresas privadas, puede considerarse una buena práctica. Esto indica un cumplimiento alto en normativa europea e internacional, aunque no necesariamente completo desde una perspectiva técnica basada en certificaciones.

La adopción de herramientas tecnológicas específicas representa un pilar fundamental para sostener una estrategia de ciberseguridad robusta en plataformas de alcance global como Booking.com. El uso de firewalls de nueva generación y sistemas IDS/IPS (detección y prevención de intrusiones), como Cisco Firepower o Palo Alto Networks, es ampliamente considerado un estándar de la industria para proteger los perímetros de red y detectar tráfico sospechoso. Aunque Booking.com no detalla públicamente la arquitectura exacta de sus sistemas de defensa, por su tamaño, madurez tecnológica y su operativa a escala mundial, es razonable suponer que cuenta con firewalls avanzados y sistemas IDS/IPS en su infraestructura central. Sin embargo, la principal dificultad reside en que estos mecanismos no se extienden a los dispositivos y redes de los hoteles colaboradores, que muchas veces no cuentan con ningún tipo de protección perimetral avanzada. Esto genera una brecha en la defensa global, ya que los ataques suelen comenzar precisamente en esos puntos externos más vulnerables.

Otra herramienta clave para la ciberseguridad es la implementación de plataformas SIEM (Security Information and Event Management), como Splunk o IBM QRadar. Estas soluciones permiten una monitorización continua de los sistemas, correlacionan eventos en tiempo real y ayudan a detectar incidentes complejos antes de que escalen. Dado que Booking.com gestiona millones de transacciones y accesos diarios, es prácticamente obligatorio que utilice alguna forma de SIEM en sus sistemas internos para garantizar un monitoreo eficaz. A pesar de esto, los ataques detectados dentro de su sistema de

mensajería en años recientes muestran que la capacidad de detección proactiva aún tiene margen de mejora, especialmente si los puntos de entrada inicial provienen de credenciales comprometidas de hoteles, fuera del alcance del SIEM central. Esto sugiere una falta de integración entre el monitoreo interno de la plataforma y la seguridad de sus socios.

Respecto a la capacitación continua y la sensibilización ante amenazas, el uso de simuladores de phishing como KnowBe4 o Cofense ha demostrado ser una medida eficaz para reducir el éxito de los ataques de ingeniería social. Booking.com, sin embargo, ha sido blanco de múltiples campañas de phishing que se han ejecutado con éxito precisamente a través de la interfaz de comunicación de la propia plataforma, usando cuentas de hoteles comprometidas. La reiteración de este tipo de ataques, muchos de ellos detectados solo después de afectar a múltiples usuarios, indica que no se ha desarrollado aún un programa sistemático de formación ni se emplean de forma consistente simuladores con socios externos. Esto evidencia que el componente humano sigue siendo el eslabón más débil de su cadena de seguridad. A pesar de que es probable que el personal interno de Booking.com reciba capacitación básica, no hay evidencia de que esta formación se extienda con regularidad ni con métodos interactivos a los empleados de los alojamientos asociados.

En cuanto a las arquitecturas de acceso, uno de los paradigmas más sólidos actualmente es la Zero Trust Architecture, que parte del principio de que no se debe confiar automáticamente en ningún usuario o dispositivo, ni siquiera dentro de la red interna. Este enfoque requiere autenticación continua, control de acceso granular y segmentación de red. Aunque Booking.com ha implementado mejoras como la autenticación en dos pasos y mayores controles de acceso tras algunos incidentes, la continuidad de los ataques de suplantación a través de cuentas legítimas de hoteles indica que el modelo de Zero Trust aún no está plenamente desplegado, especialmente en lo que respecta al entorno extendido fuera de su red central. Los ciberdelincuentes han podido moverse lateralmente dentro del sistema una vez que acceden a través de una cuenta comprometida, lo cual es precisamente lo que una arquitectura Zero Trust busca impedir. Por tanto, si bien puede haber pasos iniciales hacia este enfoque, aún no se puede afirmar que esté implementado de forma madura o integral.

Finalmente, la protección de APIs es un componente esencial en empresas con arquitecturas modernas basadas en microservicios, como es el caso de Booking.com.

Herramientas como Salt Security o Imperva API Security permiten controlar el tráfico de interfaces programáticas, identificar usos anómalos y evitar accesos no autorizados o abusivos. En este sentido, la propia documentación técnica de vulnerabilidades reportadas en años recientes sugiere que las APIs de Booking.com han presentado problemas de configuración o falta de validaciones adecuadas, facilitando filtraciones de datos. Por ejemplo, el caso reportado en 2024, donde información de reservas fue expuesta por una mala configuración de un servidor externo, podría haberse evitado con una supervisión más estricta del uso de APIs. Estos incidentes muestran que, si bien probablemente existan controles básicos, aún falta una estrategia avanzada y automatizada de protección de interfaces, como la que proporcionan las herramientas líderes del mercado.

2.4.2. Gestión de datos personales y medidas de protección en Booking.com

La gestión adecuada de los datos personales constituye uno de los pilares fundamentales para construir confianza en el entorno digital, especialmente en sectores como el turismo, donde las plataformas recogen, procesan y almacenan grandes volúmenes de información sensible de millones de usuarios en todo el mundo. En este contexto, Booking.com ha tenido que adaptar sus prácticas a un marco normativo cada vez más exigente, al tiempo que responde a las expectativas crecientes de los consumidores en materia de privacidad. Uno de los primeros indicadores clave para evaluar el nivel de cumplimiento en este ámbito es la tasa de solicitudes de ejercicio de derechos RGPD, como acceso, rectificación, supresión o portabilidad de datos, atendidas dentro del plazo legal de 30 días (TrustCommunity, 2025). Aunque la empresa no publica informes detallados sobre este punto, desde la entrada en vigor del Reglamento General de Protección de Datos (RGPD) en 2018, Booking.com ha implementado mecanismos en su interfaz que permiten a los usuarios gestionar sus datos de forma directa, lo cual sugiere que existe al menos una infraestructura funcional para cumplir este requisito. No obstante, se han registrado quejas aisladas de usuarios en foros y redes sociales sobre retrasos o falta de claridad en la gestión de estos derechos, lo que indica que, aunque el cumplimiento es probablemente alto, no siempre se alcanza el 100 % esperado.

Otro aspecto esencial es el nivel de transparencia de las políticas de privacidad. Este indicador se relaciona con la claridad del lenguaje utilizado, la facilidad de acceso al contenido y la comprensión general por parte del usuario medio. En este punto, Booking.com ha realizado avances significativos en los últimos años. Sus políticas están disponibles en múltiples idiomas, utilizan un lenguaje relativamente accesible y están

organizadas en secciones que explican qué datos se recogen, con qué finalidad y durante cuánto tiempo. Asimismo, se incluyen descripciones sobre transferencias internacionales de datos y sobre los derechos del usuario, lo cual refleja una voluntad de adaptación a los principios de transparencia. Sin embargo, la experiencia del usuario varía según el país y el nivel de alfabetización digital, por lo que sería recomendable que la empresa complementara estas políticas con recursos explicativos interactivos o materiales de apoyo para usuarios menos familiarizados con los términos legales. En términos generales, puede decirse que Booking.com cumple razonablemente bien este indicador, aunque aún hay margen para mejorar la accesibilidad y comprensibilidad real de la información.

En cuanto a la frecuencia de auditorías del tratamiento de datos, las mejores prácticas internacionales recomiendan realizar al menos dos revisiones formales por año, especialmente en empresas que gestionan datos personales a gran escala. Aunque Booking.com no ha revelado públicamente el número exacto de auditorías realizadas anualmente, su tamaño, su exposición a marcos regulatorios exigentes como el RGPD, la CCPA (California Consumer Privacy Act) o la LOPDGDD en España, y su historial reciente con sanciones como la multa de 475.000 euros en 2018, sugieren que la empresa ha debido reforzar su programa de control interno. No obstante, algunos incidentes posteriores, como la filtración de datos en 2024 por mala configuración de servidores externos, ponen en duda la eficacia o la profundidad de dichas auditorías. Se infiere, por tanto, que las auditorías se realizan, pero que su calidad o capacidad de anticipación aún pueden ser optimizadas (LevelBlue, 2024).

El uso de técnicas de minimización y anonimización de datos sensibles es otro de los pilares fundamentales de un tratamiento ético y legal de la información personal. La minimización de datos implica recopilar únicamente la información necesaria para cumplir un propósito determinado, mientras que la anonimización busca disociar los datos de los individuos para evitar que sean identificables. Booking.com ha avanzado en este sentido, particularmente desde la entrada en vigor del RGPD, adoptando medidas como la eliminación progresiva de datos no esenciales, la restricción del acceso interno a información crítica y el uso de herramientas de cifrado. También ha manifestado su intención de avanzar hacia sistemas de anonimización y seudonimización más robustos, especialmente en sus análisis masivos de datos (big data). Sin embargo, casos como la exposición de itinerarios y datos personales sin cifrar en ciertos ataques indican que estas

técnicas no siempre se aplican de manera uniforme o completa en todo el ciclo de vida del dato. Por tanto, puede considerarse que existe un cumplimiento parcial con una clara intención de mejora.

En relación con el cumplimiento normativo, Booking.com se encuentra bajo la jurisdicción de marcos como el RGPD, la LOPDGDD y la CCPA, entre otros. El cumplimiento de estas leyes requiere no solo ajustarse a requisitos técnicos, sino también mantener un historial limpio de sanciones. En este aspecto, la plataforma ha tenido algunas dificultades: la sanción recibida en 2021 por su tardía notificación de una brecha de seguridad demuestra que el cumplimiento ha sido imperfecto en el pasado. Sin embargo, desde entonces, la empresa ha intensificado sus esfuerzos por alinearse con las normativas aplicables, incluyendo mejoras en sus procesos de notificación y en la gestión del consentimiento. En los últimos años, no se han documentado sanciones graves adicionales, lo que sugiere una evolución positiva hacia el cumplimiento continuo. Aun así, el historial previo implica que el indicador no puede considerarse totalmente cubierto a lo largo del periodo reciente.

Finalmente, el porcentaje de terceros que acceden a datos personales bajo cláusulas contractuales estandarizadas es esencial para proteger la información compartida con proveedores, alojamientos y servicios tecnológicos asociados. El RGPD exige que toda cesión de datos a terceros esté respaldada por contratos específicos que regulen las responsabilidades y los niveles de protección requeridos. En este sentido, Booking.com declara en sus políticas de privacidad que todos los terceros con los que colabora están sujetos a condiciones contractuales que garantizan un nivel adecuado de protección, incluyendo el uso de cláusulas tipo aprobadas por la Comisión Europea cuando los datos son transferidos fuera del Espacio Económico Europeo. Aunque no existe verificación pública de la totalidad de estos acuerdos, la inclusión sistemática de estas referencias en su documentación legal y su adhesión al marco europeo permiten inferir un nivel de cumplimiento alto, cercano al 100 %.

En el caso de Booking.com, cuya actividad implica la recolección y procesamiento de información personal y financiera de millones de usuarios a nivel mundial, contar con soluciones especializadas no es solo recomendable, sino imprescindible. Las plataformas de gestión de privacidad, como OneTrust o TrustArc, permiten a las organizaciones coordinar y automatizar el cumplimiento de normativas como el RGPD o la CCPA, gestionando solicitudes de usuarios, evaluaciones de impacto (PIA/DPIA),

consentimientos y políticas de cookies. Aunque Booking.com no ha comunicado públicamente el uso de estas herramientas específicas, su presencia en países regulados y su declaración de cumplimiento normativo sugieren que utiliza algún tipo de plataforma de gestión interna que cumple funciones similares. No obstante, la ausencia de referencias directas a OneTrust, TrustArc u otras plataformas líderes deja abierta la posibilidad de que la solución adoptada no esté alineada con los estándares más robustos y transparentes del mercado.

El uso de sistemas de cifrado tanto en tránsito como en reposo es otra medida indispensable para preservar la confidencialidad e integridad de los datos personales. Tecnologías como AWS Key Management Service (KMS) o Microsoft Azure Key Vault permiten cifrar datos sensibles con claves seguras y gestionar el acceso de forma controlada. Booking.com declara en sus políticas que emplea mecanismos de cifrado para proteger los datos de los usuarios, especialmente los financieros, y ha adoptado prácticas como el uso de pasarelas de pago externas (Stripe, PayPal, Redsys) que garantizan que la información crítica no quede almacenada directamente en sus servidores. Esta decisión técnica es coherente con las recomendaciones internacionales y refleja un enfoque correcto. Sin embargo, el historial de incidentes sugiere que, en ciertos entornos, como servidores gestionados por terceros o sistemas externos vinculados a hoteles, no siempre se han aplicado correctamente estas medidas, lo cual ha permitido filtraciones puntuales. Por tanto, puede afirmarse que el cifrado es una práctica aplicada por la plataforma, aunque con margen de mejora en entornos descentralizados o compartidos.

Otro elemento esencial en la gestión moderna de la privacidad es la disponibilidad de dashboards de consentimiento y herramientas de gestión de cookies que sean accesibles, configurables y comprensibles por el usuario. Booking.com ofrece actualmente un panel de cookies donde los visitantes pueden modificar sus preferencias, rechazar el uso de tecnologías de seguimiento no esenciales y consultar la finalidad de cada categoría de cookie. Esta funcionalidad se encuentra integrada en su política de privacidad y cumple, en principio, con los requisitos mínimos del RGPD. Aun así, algunos usuarios han señalado que el diseño no siempre es intuitivo o completamente claro, y que las opciones predeterminadas tienden a favorecer la activación de cookies, lo cual puede ser interpretado como una forma de consentimiento implícito. Por consiguiente, aunque se ha avanzado en el cumplimiento formal, aún existe la necesidad de mejorar la experiencia del usuario en términos de transparencia y control real.

En lo que respecta al uso de herramientas de anonimización y seudonimización, como ARX Data Anonymization Tool, su importancia radica en la posibilidad de realizar análisis de datos sin comprometer la identidad de los individuos. Booking.com ha manifestado su intención de avanzar hacia la minimización del dato y el uso ético de técnicas de anonimización, especialmente en el contexto del big data y la personalización de servicios. Sin embargo, no hay información pública detallada sobre las herramientas específicas que utiliza ni sobre la metodología de anonimización aplicada. Además, varios incidentes han demostrado que los datos personales expuestos incluían nombres, itinerarios, teléfonos y direcciones, lo cual indica que, al menos en algunos sistemas, la anonimización no se ha llevado a cabo de forma efectiva o no se ha implementado en todos los niveles. Este vacío revela una debilidad potencial en la gestión de datos secundarios o históricos, donde muchas organizaciones suelen relajar sus estándares de seguridad.

Por último, el uso de sistemas de prevención de fuga de datos (Data Loss Prevention, DLP) como los ofrecidos por Symantec o Forcepoint es vital para evitar que información confidencial salga de los entornos autorizados, ya sea por error humano o por acción maliciosa. Estas herramientas monitorizan en tiempo real los flujos de datos, bloquean operaciones sospechosas y alertan sobre posibles brechas. Si bien se espera que una empresa del tamaño de Booking.com emplee algún tipo de tecnología DLP para su infraestructura central, los incidentes de acceso indebido a cuentas de hoteles, la exfiltración de datos de clientes en 2018 y las filtraciones mediante phishing en 2023–2025 evidencian que la protección no ha sido total. Especialmente preocupante es el hecho de que varios ataques hayan logrado extraer información personal utilizando canales internos (como la mensajería de la plataforma), lo cual sugiere una carencia de filtros preventivos en esos entornos concretos. Aunque el sistema puede estar protegido en sus áreas críticas, las fugas de información asociadas a socios externos indican que la cobertura de DLP no se extiende de forma integral a toda la red de interacción.

En resumen, Booking.com ha implementado varias de las herramientas recomendadas para la protección de datos personales, como el cifrado y la gestión de cookies, y probablemente cuenta con soluciones equivalentes a las plataformas de gestión de privacidad y sistemas DLP en su infraestructura central. Sin embargo, su principal debilidad sigue siendo la falta de uniformidad en la aplicación de estas herramientas más allá de su núcleo corporativo. En los espacios donde interactúan sus socios hoteleros y

proveedores externos, persisten vulnerabilidades que no han sido cubiertas plenamente por tecnologías como la anonimización efectiva, la protección de datos en entornos compartidos o los sistemas de detección proactiva de filtraciones. Esto revela la necesidad urgente de extender el uso de herramientas avanzadas a toda la cadena operativa, no solo para garantizar el cumplimiento legal, sino también para proteger la reputación y la confianza de millones de usuarios que dependen de la plataforma.

3. Conclusiones y recomendaciones

La ciberseguridad no puede entenderse solo desde un enfoque técnico, sino como un componente estructural de la experiencia digital, tal como se expuso en la primera parte del presente trabajo y los conceptos de confidencialidad, integridad, disponibilidad, autenticación, autorización y gestión del riesgo, desarrollados teóricamente, se manifiestan en la realidad de empresas como Booking.com de manera concreta. Las múltiples brechas analizadas muestran que la protección de los datos personales no depende únicamente de herramientas tecnológicas, sino también de los procesos organizativos y, sobre todo, del factor humano, el más vulnerable de los tres pilares de la ciberseguridad. Además, se ha evidenciado que los fallos de coordinación con los socios hoteleros y la falta de formación en estos actores externos son una amenaza real para la continuidad del negocio, reflejando la teoría según la cual la confianza digital no se construye solo con firewalls, sino con políticas, comunicación y cultura organizacional. El usuario confía en la plataforma no porque entienda sus sistemas, sino porque percibe coherencia entre la promesa de privacidad y su experiencia real. Cuando esa coherencia falla, como en los casos de phishing o filtraciones, la reputación digital se ve comprometida, afectando la lealtad del cliente, tal como se explicó en el apartado teórico inicial.

Desde un punto de vista normativo, queda en relieve la importancia del cumplimiento formal de marcos regulatorios como el RGPD y el Esquema Nacional de Seguridad. La teoría jurídica que sitúa al consentimiento, la minimización de datos y la transparencia como ejes de la protección de la privacidad toma especial relevancia ante las sanciones y críticas que ha enfrentado la empresa en los últimos años.

El caso de Booking.com, que se ha analizado a lo largo del presente trabajo, sirve como ejemplo claro de cómo los principios de ciberseguridad se deben reflejar en medidas integradas, sostenidas y cooperativas pero, sobre todo, efectivas. La teoría analizada al inicio no es solo un marco de referencia, sino una hoja de ruta práctica que permite comprender, anticipar y corregir los fallos que comprometen tanto la seguridad técnica como la confianza del usuario. Por ello, este trabajo no solo ha evaluado el desempeño de una empresa concreta, sino que estaría reafirmando la vigencia y aplicabilidad del marco teórico existente en un entorno digital cada vez más complejo, interconectado y regulado.

El análisis realizado sobre la evolución de la ciberseguridad y la gestión de datos personales en Booking.com pone de manifiesto una realidad dual: por un lado, existe un notable esfuerzo por parte de la plataforma en cumplir con las normativas internacionales más exigentes, implementar tecnologías de protección avanzadas y desarrollar políticas de privacidad cada vez más transparentes; pero, por otro, persisten importantes brechas operativas y organizativas, especialmente en la relación con sus socios hoteleros y en la gestión extendida de sus infraestructuras.

De todo lo expuesto se pueden extraer las siguientes conclusiones, que dan respuesta a los objetivos planteados en apartados anteriores del presente trabajo:

- La ciberseguridad debe abordarse desde una perspectiva integral que combine tecnología, procesos y personas, siendo el factor humano el más propenso a errores y vulnerabilidades.
- La confianza digital es un elemento esencial en el entorno online, y se construye a través de prácticas de seguridad sólidas, comunicación transparente y cumplimiento normativo efectivo.
- El marco legal europeo, especialmente el RGPD, establece principios como la minimización de datos, el consentimiento explícito y la rendición de cuentas, que deben guiar todas las estrategias de protección de la información.
- Booking.com ha presentado varios problemas de ciberseguridad a lo largo de su actividad empresarial y han sido detallados en apartados previos del presente trabajo.
- Booking.com cumple formalmente con normativas como el RGPD en aspectos clave: políticas de privacidad transparentes, cifrado de datos y cláusulas contractuales con terceros. Sin embargo, persisten incumplimientos como la falta de implementación obligatoria de la autenticación multifactor (MFA), la respuesta tardía ante incidentes críticos y la insuficiente formación contra phishing en socios hoteleros.

Para dar respuesta al último objetivo planteado en el trabajo que se presenta, y a modo de conclusión, se han establecido una serie de recomendaciones estratégicas que permitirían a Booking.com fortalecer sus prácticas tanto en ciberseguridad como en privacidad:

1. Ampliar y estandarizar la implementación de medidas de seguridad en toda su red de colaboradores, especialmente en los establecimientos hoteleros. Esto implica

establecer mínimos obligatorios en protección de dispositivos, cifrado, MFA y detección de intrusiones.

2. Desarrollar un programa sistemático de formación continua en ciberseguridad, dirigido no solo a su personal interno, sino también a los empleados de hoteles y proveedores externos, priorizando temas como el reconocimiento del phishing, la gestión segura de credenciales y el manejo responsable de la información del cliente.
3. Incorporar herramientas avanzadas de anonimización, seudonimización y prevención de fuga de datos (DLP) en todos los niveles de la plataforma, incluyendo sus integraciones con socios externos, con el fin de limitar al máximo la exposición de datos sensibles.
4. Realizar auditorías de seguridad y de cumplimiento normativo al menos dos veces al año, con carácter independiente y con seguimiento explícito de sus resultados y medidas correctivas.
5. Adoptar un modelo de arquitectura Zero Trust de forma progresiva, garantizando que ningún usuario o sistema tenga acceso más allá del estrictamente necesario, independientemente de su posición en la red.
6. Mejorar la experiencia del usuario en la gestión del consentimiento, haciendo los paneles de privacidad más comprensibles, visuales e intuitivos, evitando patrones oscuros y promoviendo el control activo por parte del usuario sobre sus propios datos.
7. Publicar de forma transparente información sobre sus certificaciones y herramientas específicas utilizadas, como ISO/IEC 27001, OneTrust, TrustArc, ARX u otras, para reforzar su reputación y facilitar la evaluación externa de su compromiso con la protección de datos.

Booking.com se encuentra en un punto de madurez tecnológica alto, aunque su modelo de negocio interconectado y su dependencia de redes de terceros introducen riesgos significativos que deben ser abordados desde una lógica de corresponsabilidad. No basta con proteger los sistemas centrales de la empresa; resulta imprescindible adoptar un enfoque de ciberseguridad distribuida, donde todos los actores implicados, incluidos socios hoteleros, proveedores tecnológicos y usuarios finales, participen activamente en la protección del entorno digital. Esto implica establecer estándares comunes de

seguridad, garantizar una supervisión más efectiva de las integraciones externas y promover la rendición de cuentas en cada eslabón de la cadena operativa.

Una ciberseguridad verdaderamente eficaz no puede limitarse a soluciones tecnológicas puntuales o reactivas, sino que debe ser preventiva, dinámica y adaptativa, tal y como se desprende de los principios analizados en la parte teórica de este trabajo. En este sentido, resulta esencial fortalecer la cooperación activa entre las distintas unidades internas de la empresa, fomentar una cultura de seguridad centrada en la formación continua y dotar a los usuarios y colaboradores de herramientas que les permitan tomar decisiones informadas respecto a la privacidad y la gestión de sus datos. Además, la confianza digital. concepto clave en el ecosistema online, no se construye exclusivamente con firewalls o cifrado, sino también con transparencia institucional, respuestas ágiles ante incidentes y un compromiso sostenido con el respeto a los derechos fundamentales de los usuarios. La experiencia de Booking.com demuestra que, a pesar de cumplir con buena parte de la normativa vigente, aún existen áreas críticas donde la mejora es urgente: brechas en la comunicación con socios externos, falta de uniformidad en las prácticas de seguridad y una escasa proactividad ante amenazas persistentes como el phishing dirigido.

En este escenario, la ciberseguridad deja de ser un requisito técnico y pasa a constituir una estrategia de marca, una ventaja competitiva capaz de generar fidelidad y diferenciación en un mercado saturado. Booking.com, como líder en el sector turístico digital, tiene la capacidad y la responsabilidad de convertirse en un referente no solo por la eficacia de sus servicios, sino también por la solidez ética y técnica de su gestión de datos. Consolidarse como una plataforma segura, confiable y resiliente implica adoptar un modelo de gobernanza más ambicioso, alineado con los estándares más exigentes a nivel internacional, como la arquitectura Zero Trust, la certificación ISO/IEC 27001 o las metodologías de privacidad desde el diseño. Solo mediante una combinación coherente de tecnología avanzada, políticas responsables y una visión humanista de la seguridad digital, podrá Booking.com garantizar no solo el cumplimiento legal, sino también la legitimidad social de su actividad. Así, más allá de proteger sus activos, estará protegiendo el vínculo de confianza que sostiene a millones de relaciones comerciales a diario. Esa será, en última instancia, la base de su sostenibilidad a largo plazo en un entorno cada vez más regulado, competitivo y consciente de los riesgos que entraña el mundo digital.

AGRADECIMIENTOS

En primer lugar, agradecer a la Facultad de Ciencias Sociales y Juridicas de Orihuela por darme la oportunidad de estudiar esta carrera, con la que he aprendido entro otros muchos conocimientos, sobre el ámbito de marketing, a través de dichos conocimientos he podido desarrollar este trabajo.

Agradezco a las personas que me han ayudado a llega a este punto, como han sido mis compañeros de clase y profesores, destacar que he tenido mucha suerte de conocer gente maravillosa a lo largo de este periodo, sin ellos no habría sido posible.

Agradecer especialmente a mi tutor Don José Francisco Parra Azor, por darme la oportunidad de trabajar con él y hacerme fácil este trabajo.

También agradecer a mi familia, especialmente a mi madre sin su apoyo y paciencia no habría podido llegar al final de este proyecto.

4. Bibliografía

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and Human Behavior in the Age of Information. *Science*, *347*(6221), 509-514.
2. Booking.com. (2025, marzo). Política de privacidad y cookies. https://www.booking.com/content/privacy.es.html
3. Booking.com. (n.d.). Privacy Notice & Cookie Statement. https://www.booking.com/pipl_privacy_statement.en-gb.html
4. Borky, J. M., & Bradley, T. H. (2018). Effective model-based systems engineering. In J. M. Borky & T. H. Bradley (Eds.), *Model-based systems engineering: Theory and application* (pp. 345–404). Springer. https://doi.org/10.1007/978-3-319-95669-5_10
5. Cimpanu, C. (2021, 30 de marzo). Booking.com fined €475,000 for reporting data breach too late. *The Record from Recorded Future News*. https://therecord.media/booking-com-fined-e475000-for-reporting-data-breach-too-late
6. ClickFix phishing scam targets Booking.com users. (2023, 5 de octubre). *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/clickfix-phishing-scam-booking/
7. Cuidado si recibes un mensaje extraño en nombre de tu hotel a través del chat de Booking. (2024, 9 de febrero). *Maldita.es*. https://maldita.es/timo/bulo/20240209/booking-chat-hotel-reserva/
8. Del-Real, C., & Díaz-Fernández, A. M. (2022). Understanding the plural landscape of cybersecurity governance in Spain: A matter of capital exchange. *International Cybersecurity Law Review*, *3*(2), 313–343. https://doi.org/10.1365/s43439-022-00069-4
9. Europa Press. (2025, 14 de marzo). Suplantan a Booking en una campaña de 'phishing' dirigida contra profesionales hoteleros y de viajes. *La Vanguardia*. https://www.lavanguardia.com/ciencia/20250314/10479933/suplantan-booking-campana-phishing-dirigida-profesionales-hoteleros-viajes-ep-agenciaslv20250314.html
10. European Data Protection Board. (2020, 24 de abril). Dutch SA fines Booking.com for delay in reporting data breach. https://www.edpb.europa.eu/news/national-news/2020/dutch-sa-fines-bookingcom-delay-reporting-data-breach_en
11. Fake Booking.com messages cost hotels more than money. (2025, 5 de junio). *Hospitality.today*. https://www.hospitality.today/article/fake-booking-com-messages-cost-hotels-more-than-money
12. Hetzmann, M. (2025, 26 de febrero). Enorme estafa de phishing en Booking.com: usuarios húngaros perdieron enormes cantidades de dinero. *HolaMagyar*. Recuperado de https://holamagyar.hu/enorme-estafa-de-phishing-en-booking-com-usuarios-hungaros-perdieron-enormes-cantidades-de-dinero/
13. Hotel hackers redirect guests to fake Booking.com to steal cards. (2023, 22 de septiembre). *BleepingComputer*. https://www.bleepingcomputer.com/news/security/hotel-hackers-redirect-guests-to-fake-bookingcom-to-steal-cards/
14. Kaaij, M. van der, & Dohmen, J. (2021, 10 de noviembre). American spy hacked Booking.com, company stayed silent. *NRC*. https://www.nrc.nl/nieuws/2021/11/10/american-spy-hacked-bookingcom-company-stayed-silent-a4065086

15. Knaus, C. (2024, 31 de enero). Booking.com scams surge in Australia, ACCC warns. *The Guardian*. https://www.theguardian.com/australia-news/2024/jan/31/bookingcom-scams-surge-australia-accc
16. LevelBlue. (2024, 22 de marzo). *How often should security audits be?* https://levelblue.com/blogs/security-essentials/how-often-should-security-audits-be
17. Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce.*Frontiers in Psychology, 13*, 927398. https://doi.org/10.3389/fpsyg.2022.927398
18. Mahboub, O., & El-Kourdi, I. (2024). Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks: A qualitative study. *World Journal of Advanced Research and Reviews, 23*(03), 443–452. https://wjarr.com/sites/default/files/WJARR-2024-2538.pdf
19. Microsoft. (2025, 13 de marzo). Una campaña de phishing suplanta a Booking.com y distribuye malware para robar credenciales. *Microsoft News*. https://news.microsoft.com/es-es/2025/03/13/una-campana-de-phishing-suplanta-a-booking-com-y-distribuye-malware-para-robar-credenciales/
20. Nawaz, N. A., Ishaq, K., Farooq, U., Khalil, A., Rasheed, S., Abid, A., & Rosdi, F. (2023). A comprehensive review of security threats and solutions for the online social networks industry. *PeerJ Computer Science*, *9*, e1143. https://doi.org/10.7717/peerj-cs.1143
21. Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Papers (CSWP). https://doi.org/10.6028/NIST.CSWP.29
22. Perception Point. (2023, 27 de septiembre). Booking.com Customers Hit by Phishing Campaign Delivered Via Compromised Hotels Accounts. https://perception-point.io/blog/booking-com-customers-hit-by-phishing-campaign-delivered-via-compromised-hotels-accounts/
23. Phishing attacks through booking.com's own platform. (n.d.). [Publicación de Reddit]. En *r/Bookingcom*. Reddit. https://www.reddit.com/r/Bookingcom/comments/1jdhcve/phishing_attacks_through_bookingcoms_own_platform/
24. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors (Basel)*, *23*(15), 6666. https://doi.org/10.3390/s23156666
25. Salt Security. (2023, 3 de febrero). Salt Security Uncovers API Security Flaws Within Booking.com That Allowed Full Account Takeover; Issues Have Been Remediated. https://salt.security/press-releases/salt-security-uncovers-api-security-flaws-within-booking-com-that-allowed-full-account-takeover-issues-have-been-remediated
26. Schwartz, P. M., & Solove, D. J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *NYU Law Review*, *86*(6). https://nyulawreview.org/issues/volume-86-number-6/the-pii-problem-privacy-and-a-new-concept-of-personally-identifiable-information/
27. SES Hospedajes. (2025, 20 de abril). Guía completa para alojamientos y rent a car: Cómo cumplir con SES.Hospedajes sin perder la cabeza. https://seshospedajes.es/guia-completa-2025-ses-hospedajes/

28. TrustCommunity. (2025, 10 de abril). *GDPR compliance: A comprehensive guide for businesses in 2025*. https://community.trustcloud.ai/article/gdpr-compliance-a-comprehensive-guide-for-businesses/
29. Vertiz-Aguirre, J. (2023). *La transformación digital en las empresas turísticas de alojamiento* [Trabajo Fin de Máster, Universidad de Málaga]. https://riuma.uma.es/xmlui/bitstream/handle/10630/28403/TFM_Vertiz%2C%20Jaione.pdf?sequence=1