- **Expediente N.º: EXP202309952**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 25 de mayo de 2023, se presentó reclamación con número de registro de entrada REGAGE23e00033334938 ante la Agencia Española de Protección de Datos que pone de manifiesto una posible infracción imputable a MEDANO4YOU, S.L. (en adelante, MEDANO). Los motivos en que basa la reclamación son los siguientes:

La reclamante realizó una reserva del alojamiento "***(…)* - by MEDANO4YOU**", a través de booking.com. Con fecha 29/03/2023 recibió, desde una línea móvil británica, mensajes de WhatsApp en el que alguien, presuntamente en nombre del alojamiento y conociendo datos personales suyos (nombre, dirección de e-mail, teléfono, número de reserva y alojamiento reservado). Recibió un primer mensaje de bienvenida y un segundo mensaje en el que se le comunicaba una supuesta incidencia en relación con la reserva, pidiéndole que confirmara los datos de pago accediendo a un correo electrónico que contenía un enlace que resultó ser fraudulento.

La reclamante se puso en contacto con MEDANO, responsable del alojamiento. A través del servicio de mensajería de Booking.com, MEDANO le indicó que se había detectado una amenaza de fraude, le advertía que no facilitara sus datos si recibía un mensaje a través de Booking.com y le facilitaba un teléfono alternativo de contacto. El 09/04/2023, la reclamante interpuso denuncia por los hechos ante la Policía Nacional.

Junto a la notificación se aportan mensajes de WhatsApp fraudulentos, mensaje de MEDANO alertando del fraude y atestado de la Policía Nacional nº ***REFERENCIA.1** con la denuncia.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a MEDANO, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), se realizó mediante notificación electrónica, que fue puesta a disposición el 14/07/2023 y aceptada el 17/07/2023. No se recibió respuesta a este escrito de traslado.

TERCERO: Con fecha 25/08/2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Requerida para informar sobre el funcionamiento de reservas, MEDANO manifiestó lo siguiente:

> "*Medano4you, S.L., es una empresa que se dedica a gestionar viviendas de muchos propietarios y explotar el alquiler y el turismo vacacional de las mismas. Las personas que se quieren quedar en las viviendas que gestionan pueden reservar por diferentes formas, Booking, Airbnb o su propia plataforma medano4you.com.*
> (…)
> *Los datos se procesan por Booking.com, como se ha indicado y se transmiten al establecimiento por medio de un mensaje con ciertos datos, pero no todos. Es Booking el responsable principal de los datos. El establecimiento recibirá todos los datos necesarios del huésped en el momento de hacer el cheking."*

Sobre el traslado de información entre Booking.com y el alojamiento, según las manifestaciones aportadas la operativa de trabajo consistiría en el empleo de un software de gestión de una tercera parte, KROSS BOOKING, que se conecta a los servicios de terceros, como Booking.com, y procesa y traslada la información para que pueda ser atendida por el personal del establecimiento. Adicionalmente, el alojamiento recibe un correo electrónico con los datos de la reserva. Respecto del uso del software de gestión que actúa de intermediario entre la plataforma de Booking.com y los dispositivos locales, MEDANO afirma que se trata de un proceso automático y aporta documentación sobre la gestión de la privacidad en esta herramienta.

Este tratamiento por parte del establecimiento se realizaría fuera del entorno de la plataforma de Booking.com, tal como se manifiesta por la parte reclamada: "*Se almacenan en sus propios servidores que no se han visto amenazados por la incidencia, ni por ninguna otra.*" Adicionalmente, se emplearían hojas de cálculo almacenadas localmente en los dispositivos del alojamiento: "*lo que se almacena en los ordenadores es la transcripción de ese software mediante hojas de cálculo*".

Por otra parte, la parte reclamada manifiesta lo siguiente sobre el uso que hace de la plataforma de Booking.com:

> "*Se usan tres ordenadores para acceder a Booking, solo tres, precisamente porque según la administradora es muy difícil emparejar un nuevo ordenador. Por otro lado, solo acceden a Booking para descargarse las facturas con la plataforma y para dar de alta una vivienda nueva. En el día a día no acceden a la cuenta, porque no lo necesitan para el ejercicio de las funciones diarias."*

En cualquier caso, aunque la parte reclamada no acceda a Booking.com directamente, es independiente a que se puedan recibir reservas de nuevos clientes mediante esa plataforma y que se realice el volcado de datos mediante el software de gestión.

En el marco de las actuaciones previas de investigación se ha requerido información a BOOKING.COM, B.V. (en adelante, BOOKING), a través de la Autoridad de control de Países Bajos. De acuerdo con BOOKING (se traduce la respuesta):

> "*A través de una cuenta, solo se pueden ver las reservas de los alojamientos a los que tiene acceso esa cuenta. Esto significa que la cuenta no se puede utilizar para ver las reservas realizadas por un cliente en alojamientos no vinculados a la cuenta. Además, a través de una cuenta, solo se pueden ver los detalles de la reserva de un solo huésped utilizando la funcionalidad de búsqueda para las reservas pertenecientes a los alojamientos a los que tiene acceso, y solo para las reservas no archivadas. Un proveedor de alojamiento no puede elegir un huésped y ver su historial de reservas de forma agregada o de cualquier otra manera.*"

En base a eso, una posible brecha de seguridad que afectase a un alojamiento quedaría limitada al ámbito de ese establecimiento y la plataforma, no pudiendo ser ocasionada por un tercer alojamiento ajeno dado de alta en la plataforma.

MEDANO informa de que el incidente y fraude a la parte reclamante se enmarca en una brecha de seguridad que afectó a más clientes, que recibieron intentos de estafa análogos al denunciado. Si bien en el caso denunciado la comunicación fraudulenta se realizó empleando WhatsApp y correo electrónico, en otros casos se utilizó el sistema de mensajería propio de la plataforma de BOOKING y aporta como evidencia de este hecho diferentes mensajes, similares al de la reclamación, utilizando la plataforma. MEDANO afirma desconocer el alcance y origen y señala a la plataforma Booking.com como responsable del incidente de seguridad.

Por su parte, BOOKING manifiesta que no le consta que las cuentas que emplea MEDANO se hayan visto comprometidas en 2023. Informa que ha identificado que utilizando la cuenta de otros alojamientos hubo intentos de fraude similares y descarga la possible responsabilidad en lo alojamientos, señalando como possible causa las cuentas de éstos y los sistemas informáticos bajo el control de los usuarios de la plataforma (los alojamientos).

En el curso de las actuaciones previas de investigación no ha sido posible determinar el origen de la brecha.

En cuanto al impacto de la brecha, de acuerdo con la información facilitada por MEDANO, ascendería a 24 personas, tomando como referencia el número de clientes que fueron contactados por la mensajería de la propia plataforma de Booking.com y a los que tuvo acceso MEDANO. Una vez conocido el incidente, MEDANO informó a los posibles afectados (clientes que habían reservado sus alojamientos). Aporta ejemplos de las comunicaciones realizadas.

En cuanto a las comunicaciones mantenidas entre MEDANO y BOOKING en relación con el indicente, la primera manifiesta lo siguiente:

> "*El día 30 de marzo de 2023 y días sucesivos. Se envió correo a la comercial asignada pero como no contestó, se gestionó la incidencia de forma telefónica. Por tanto, no hay pruebas que aportar*."

En cuanto a las medidas de seguridad adoptadas antes de la brecha, ***(…).***

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Cuestiones previas

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante brecha de seguridad) como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haber tenido acceso a los datos de la reclamante un tercero que los ha utilizado para realizar un fraude.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan la seguridad del

tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Presunción de inocencia

En el presente caso, se presentó reclamación por debido a que, al verse comprometida la confidencialidad de datos personales en relación con la reserva de un alojamiento, se habría producido un intento de fraude.

De las actuaciones de investigación realizadas por esta Agencia, como se ha expuesto en los antecedentes, no ha sido posible determinar el origen de la brecha. Asimismo, no se ha acreditado una ausencia de medidas de seguridad por parte de MEDANO de la que se pueda concluir una responsabilidad en el origen de esa brecha.

A este respecto, debe destacarse que en el ámbito administrativo sancionador son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, teniendo plena virtualidad el principio de presunción de inocencia, que debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetado en la imposición de cualesquiera sanciones.

El Tribunal Constitucional en Sentencia 76/1990, considera que el derecho a la presunción de inocencia comporta "*que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio*".

De acuerdo con este planteamiento, el artículo 53.2 de la LPACAP, establece que, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables tendrán los siguientes derechos:

> "*a) (…)*
>
> *b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario."*

Como ha precisado el Tribunal Supremo en Sentencia de 26 de octubre de 1998, la vigencia del principio de presunción de inocencia

> "*no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario,*

> *irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo*."

Así las cosas, se debe distinguir la verdadera prueba de indicios de las meras sospechas o conjeturas. El Tribunal Constitucional ha manifestado en su Sentencia 24/1997, que

> "*los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que: a) La prueba indiciaria ha de partir de hechos plenamente probados. b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras).*"

En definitiva, el principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo que acredite los hechos que motivan la imputación o la intervención en los mismos del presunto infractor.

En este caso, como se ha expuesto, no existen esos indicios racionales que permitirían imputar a la parte reclamada la comisión de infracciones de la normativa de protección de datos personales, por lo que no cabe estimar enervado el derecho a la presunción de inocencia que le ampara.

IV
Conclusiones

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, al no haber sido posible atribuir la responsabilidad por el origen de la brecha, de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones

SEGUNDO: NOTIFICAR la presente resolución a MEDANO4YOU, S.L. y a la parte reclamante.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

1245-240125

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos