Expediente Nº: E/05054/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidade ***RESTO-IN GOURMET DELIVERY, S.L..*** en virtud de denuncia presentada por ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 15 de julio de 2015 tiene entrada en esta Agencia un escrito de *A.A.A.* en el que solicitan colaboración de la Agencia Española de Protección de Datos en el marco de la cooperación internacional entre las autoridades de protección de datos personales, en relación a una empresa francesa con una filial ubicada en España, conforme a lo dispuesto en el punto 6 del artículo 28 de la Directiva 95/46/CE, de 24 de octubre de 1995, que prevé que «cada autoridad pueda ser llamada a ejercer sus poderes bajo petición de otro Estado miembro».

La Comisión Nacional de Informática y Libertades efectuó una auditoría el 21 de enero de 2015 que reveló numerosos incumplimientos de la Ley n.° 78-17, de 6 de enero de 1978, modificada, relativa a la informática, a los archivos y a las libertades sobre todo en cuanto al pago en línea en la página web resto-in.fr. La empresa RESTO IN gestiona esta página de Internet y tiene su sede en París. Sin embargo, la compañía dispone de oficinas principales en Barcelona, España, donde se encuentran la mayoría de sus empleados, así como la dirección de la empresa.

Los elementos identificados en la auditoría efectuada in situ en esta sociedad a principios de este año han permitido constatar, por un lado, que la sociedad pone en marcha, en sus oficinas de Barcelona, un dispositivo de lucha contra el fraude por tarjeta bancaria. Tras verificarlo, parece que este tratamiento no ha sido objeto de ninguna autorización previa por parte de la CNIL.

Por otro lado, ha constatado que los datos bancarios (incluido el criptograma visual o código de seguridad de la tarjeta bancaria) los conserva la empresa desde el primer pago en la página web por defecto.

Por último, la empresa ha indicado haber puesto en marcha en sus bases de datos un sistema de eliminación automática de los datos conforme a las recomendaciones de la normativa española de protección de datos, pero como la administración de la base de datos tan solo se permite a los equipos ubicados en España, la CNIL no ha podido asegurarse de la veracidad de esta alegación en la auditoría in situ.

Tras analizar las actas y las constataciones hechas in situ, la CNIL ha podido identificar los siguientes incumplimientos de la Ley n.° 78-17, de 6 de enero de 1978, modificada, y de las exigencias europeas en materia de protección de datos de carácter personal:

Ausencia de información y consentimiento en cuanto al almacenamiento de cookies de la página web resto-in.fr (artículo 32-11);

Falta de información en la recopilación de datos a partir de los formularios de inscripción (artículo 32-1);

Grabación por defecto de los datos de la tarjeta bancaria y conservación del

criptograma visual de la misma (artículos 7 y 6-3e);

Puesta en marcha de un dispositivo dé lucha contra el fraude sin autorización de la CNIL (artículo 25-1-4e);

Poca exigencia de solidez de las contraseñas de los clientes, acceso al back-office de la página web en http (sin cifrado) y almacenamiento de las contraseñas en la base a través del algoritmo MD5 (artículo 34).

De las investigaciones realizadas por la CNIL se desprende que dichos tratamientos las decide y las gestiona la filial española de la sociedad, que es la única que dispone, por medio de sus servicios técnicos, de acceso a las bases de datos puestas en marcha. Tan solo se mantienen en Francia los servicios comerciales.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. En relación al almacenamiento de cookies, a través de Internet en el sitio web: http://www.resto-in.es/, se ha constatado:

- Existe una primera capa de información sobre DARD
- Existe información o enlace a información sobre DARD en la primera página.
- Utiliza DARD analíticas y de publicidad de terceros. No se ha detectado otras formas de almacenamiento local.

2. En relación a la actividad de la entidad, la empresa RESTO IN se centra en la puesta a disposición de los usuarios una plataforma web que permite intermediar entre los usuarios y restaurantes para la formalización de pedidos. RESTO IN no es el prestador de servicios ofrecidos a través de la web, sino que únicamente interviene en el perfeccionamiento de las operaciones realizadas entre los usuarios y los restaurantes prestadores de servicios. Para ello tiene suscritos convenios de colaboración con numerosos restaurantes de cada zona donde opera (Madrid, Barcelona, Paris, Marsella, Lyon, Bruselas, Berlín, Hamburgo, Londres).

El procedimiento para la captación de clientes es mediante el correspondiente formulario web, donde se informa de los Términos de Uso de la Plataforma y de las condiciones de Privacidad.

3. Los tratamientos de los datos de los clientes tanto españoles como franceses realizados por Resto In utilizan la siguiente información:

•Nombre
•Apellidos
•Dirección de e-mail y postal.
•Número de teléfono
•Pedidos realizados y lugar de los mismos.
•Fecha de caducidad de las tarjetas de crédito, tipo de tarjeta, mes y año de expiración y los últimos 4 dígitos (NO los números enteros ni los códigos de validación CSV).

•Fecha de creación de la cuenta de cliente.

•Fecha de cancelación de la cuenta de cliente.

•Empresa vinculada.

Respecto a la generación de log's de consentimientos, en la actualidad se guardan los siguientes datos de los usuarios:

I. hora de aceptación
II. IP origen de la aceptación
III. ciudad y dirección de pedido y geoposicionamiento.
IV. voluntad o no de recibir SMS y newsletter.

4. Tratamientos realizados por terceros:

La plataforma de RESTO IN utiliza pasarelas externas de pago. Una vez que el usuario ha seleccionado su menú y decide pagar, se abren dichos elementos de pago, sin que RESTO IN acceda ni conserve las claves de las tarjetas de crédito.

Los tratamientos externos que se realizan tanto con los clientes españoles como franceses son los necesarios para el cobro de las transacciones mediante las pasarelas externas.

La realización de copias de seguridad se efectúa diariamente conforme consta en el contrato de prestación de servicios vigente con la empresa de hosting.

El procedimiento para evitar el fraude en el uso de las tarjetas de crédito se fundamenta en una empresa externa, el cual es un operador con todas las garantías y que sometido a la norma de seguridad PCI DSS COMPLIANCE.

En cuanto al control del fraude en las tarjetas de crédito, se tiene suscrito el correspondiente acuerdo de colaboración.

La metodología de captación de datos de pago se fundamenta en que el mismo usuario se conecte mediante el correspondiente instrumento de pago al proveedor especializado e introduzca sus propios datos de tarjeta en dicho instrumento, no permaneciendo en los ficheros de RESTO IN datos bancarios alguno de los clientes, sólo permanece en la plataforma un número de localización de la transacción realizada y el histórico de las mismas.

El mismo procedimiento de seguridad en el pago mediante tarjeta esta implementado para todos los clientes incluidos los franceses, ya que a juicio de los representantes de Resto In, dicho procedimiento aporta todas las garantías que el estado de la técnica permite implementar.

Se ha procedido a solicitar ante la CNIL copia de la autorización de registro de ficheros estando pendiente de recibir la confirmación oficial.

6. En referencia al detalle concreto de tratamientos realizados con los números de las tarjetas bancarias, se indican los siguientes extremos:

•Información que se conserva. No se conservan los números de tarjetas, aunque si otros datos de seguridad (fecha caducidad, últimos 4 dígitos, empresa emisora) incluido un indicador de transacción.

•Los datos se conservan de forma permanente siempre que el cliente este activo. Una vez el cliente es inactivo, existe un protocolo de borrado una vez

finalizadas las obligaciones legales de conservación (5 años).

•RESTO IN no realiza tratamientos con número de tarjetas

•Información derechos ARCO. En la Web de la entidad se aporta información relativa a la política de seguridad, en la que figura "*Los usuarios podrán remitir sus solicitudes de acceso, rectificación, cancelación y oposición (en particular, para no recibir nuestras comunicaciones comerciales o para darse de baja de las eventuales suscripciones a newsletter, que se hará efectiva en un máximo de 24 horas), de conformidad con lo previsto en la LOPD, a nuestro domicilio social en Madrid, calle (C/....1) o a través de un correo electrónico a marketing@resto-in.com. En ambos casos el usuario interesado deberá acompañar una copia de su documento nacional de identidad, pasaporte u otro documento válido que lo identifique."*

5. El sistema establecido para la cancelación de los clientes es el descrito en los documentos 2 y 3 expuestos, mediante correo electrónico o postal dirigido a las direcciones indicadas.

Una vez solicitada la cancelación se procede al bloqueo de los datos del cliente y a notificar a los encargados de tratamiento de dicha cancelación.

En cuanto a las medidas de seguridad implementadas en los ficheros que contienen datos de tarjetas de crédito, tenemos que indicar que dichos ficheros no están ubicados dentro de RESTO IN, siendo responsabilidad única y exclusiva del proveedor externo.

En todos los ficheros responsabilidad de RESTO IN están implementadas las medidas de seguridad requeridas por la ley.

FUNDAMENTOS DE DERECHO

I

De conformidad con lo establecido en los artículos 37.g) y 36 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD en adelante), y en el artículo 43.1 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, (LSSI en adelante) la competencia para resolver el presente procedimiento corresponde a la Directora de la Agencia Española de Protección de Datos.

II

Es objeto de análisis en el presente procedimiento es la adecuación del sitio web www.resto-in.es/ a la normativa de protección de datos de carácter personal y la de regulación de los Servicios de la Sociedad de la Información, en concreto los principios de información, cancelación y conservación de datos, así como la información proporcionada al utilizar dispositivos de almacenamiento y recuperación de datos (DARD en adelante).

III

Dispone el **artículo 4.1 y 5 de la LOPD:** (…) *1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.(…)*

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. (…)

Dispone el **artículo 5 de la LOPD:** *1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Dispone el **artículo 16.5 de la LOPD**,: *Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado*.

IV

De las actuaciones practicadas no se desprende vulneración de los principios citados, en concreto la recogida de datos personales en la página incluye la necesaria información sobre Política de Privacidad y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

En cuanto a la política de conservación de datos, únicamente se almacenan los cuatro últimos dígitos de la tarjeta de crédito y no incluye el código CVV. Asimismo existe un procedimiento de cancelación de datos cuando el usuario se da de baja sin que se conserve información alguna derivada de las tarjetas de crédito utilizadas por los usuarios.

En relación a los pagos y el control de fraude, debe señalarse que el pago se realiza con plataformas de terceros por lo que RESTO IN ni recoge ni trata los datos relativos al pago. Y en cuanto al procedimiento de control de fraude, éste se realiza por una entidad externa en ejecución del correspondiente contrato, por lo que la entidad no interviene en dicho procedimiento.

Finalmente en cuanto a las medidas de seguridad implantadas, debe señalarse que la gestión de las contraseñas se adecua a los principios y garantías previstos en el

Titulo VIII- De las medidas de seguridad en el tratamiento de datos de carácter personal – del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

V

Es también objeto de análisis la adecuación del sitio web a lo dispuesto en el **artículo 22.2 de la LSSI** que señala que: *Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.

Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario (…)

En el presente caso se ha verificado un sistema de información ofrecido, tanto a través de una primera banda informativa como en un enlace especifico que aloja la Política de Cookies y las agrupa por finalidades y ofrece información de los principales navegadores web que impida su descarga e instalación así como información relativa a procedimientos para su eliminación.

VI

De acuerdo con lo expuesto no es posible incardinar los hechos y circunstancias puestos de manifiesto en ninguna conducta prevista en el Título VII de la LOPD y de la LSSI respectivamente, procediendo al archivo de las actuaciones.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

I.PROCEDER AL ARCHIVO de las presentes actuaciones.

II.NOTIFICAR la presente Resolución a ***RESTO-IN GOURMET DELIVERY, S.L..*** y a ***A.A.A..***

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que

se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos