

Procedimiento N°: E/08158/2019

940-0419

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: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de quiebra de seguridad remitido por **INTERCAMBIADOR DE TRANSPORTES AVENIDA DE AMERICA, S.A.U.** (en adelante ITAA) en el que informan a la Agencia Española de Protección de Datos haberse enterado por un empleado de la compañía, que recibió un mensaje de WhatsApp, de la extracción de un video captado por las cámaras del sistema de videovigilancia de las instalaciones del Intercambiador de Transportes de Avenida de América.

El video supuestamente fue extraído del sistema de videovigilancia por parte de un vigilante de seguridad de la empresa GSI Profesionales de la Seguridad y Sistemas S.A.U. (en adelante GSI), grabando directamente con su teléfono móvil la pantalla del sistema de videovigilancia.

Indican que la quiebra se produjo el 27/07/2019 y que han tenido conocimiento de ella el 31/07/2019. La notificación se ha realizado el 02/08/2019. El número de afectados es tres (dos vigilantes y un usuario del Intercambiador de Transportes). Entienden que no es necesario informar a los interesados de la existencia de la brecha de seguridad, debido a la difusión que se ha realizado de las imágenes grabadas.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de quiebra: 02 de agosto de 2019

ENTIDADES INVESTIGADAS

INTERCAMBIADOR DE TRANSPORTES AVENIDA DE AMERICA, S.A.U. con NIF A82059866 con domicilio en AV. DE AMERICA, NUM 9, PORTAL A, PISO -1, PTA. 1 - 28022 MADRID.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- HECHOS:

Realizado un requerimiento de información a ITAA, los representantes de la entidad informan de la siguiente cronología de hechos:

- Con fecha 31/07/2019, uno de los empleados de ITAA recibió la llamada de un representante del Consorcio Regional de Transportes de Madrid (en adelante "CRTM") para informarle de un incidente que había tenido lugar en las instalaciones del Responsable de Tratamiento. Acto seguido a la comunicación telefónica, el representante del CRTM envía, a través de la aplicación de mensajería instantánea WhatsApp, un vídeo en el que puede verse como uno de los vigilantes de seguridad del intercambiador de transportes de Avenida de América agrede a un usuario. Tras analizar detenidamente el vídeo recibido, se aprecia que la agresión había tenido lugar en la madrugada del día 27/07/2019 y que las imágenes que se mostraban en el vídeo habían sido captadas por una de las cámaras del sistema de videovigilancia del intercambiador de transportes de Avenida América. ITAA no tuvo conocimiento de los hechos hasta que el representante del CRTM les facilita el vídeo a través de WhatsApp.
- Después de las investigaciones realizadas, se pudo confirmar que uno de los vigilantes de la empresa GSI había grabado a través su teléfono móvil personal, y en presencia del jefe de turno que en ese momento se encontraba en la sala de control del intercambiador, las imágenes de la agresión que horas antes habían sido captadas por las cámaras de videovigilancia del intercambiador. Se desconocen los motivos por los que el vigilante de seguridad graba a través de su teléfono móvil las citadas imágenes captadas por el CCTV (Circuito Cerrado de TV - Sistema de Videovigilancia).
- Según comentarios del equipo de investigación del Grupo de Policía Judicial, el vídeo se envió a un grupo de WhatsApp en el que participan varios empleados de GSI.

En lo que respecta a la posterior propagación del vídeo, solo pueden confirmar que el vídeo se proyectó a través de redes sociales, prensa digital y televisión, desconociendo el medio o la forma en la que los diferentes medios de comunicación obtuvieron el vídeo.

- Entienden que el vídeo difundido por los medios de comunicación podría ser el grabado por el vigilante, ya que en las imágenes captadas por la cámara de videovigilancia instalada en la propia sala de control del intercambiador puede verse como el vigilante saca su teléfono móvil y enfoca hacia la pantalla del ordenador en la que se visualizan las imágenes del CCTV.

2.- MEDIDAS PREEXISTENTES:

ITAA ha aportado copia del Registro de Actividades de Tratamiento (RAT) en el que figuran los tratamientos comprometidos (sistema de videovigilancia).

La entidad ha aportado también copia del Análisis de Riesgo (AR) del tratamiento denominado "VIDEOVIGILANCIA". En el AR constan, entre otras consideraciones sobre este tratamiento:

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Responsabilidad del tratamiento				
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Bajo	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Muy bajo
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento	Sin riesgo		Sin riesgo
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento	Sin riesgo		Sin riesgo
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal	Sin riesgo		Sin riesgo

Se ha recabado copia del contrato de prestación de servicios suscrito con GSI y del contrato en materia de protección de datos firmado entre las partes en el que figura GSI como encargado. En el contrato se incluye la prestación del servicio de vigilantes de seguridad y el sistema de videovigilancia a través del CCTV. En él consta que el personal se encuentra comprometido de forma expresa y por escrito a guardar la confidencialidad.

Los representantes de ITAA informan que los vigilantes de seguridad, empleados de GSI, suscriben compromisos de confidencialidad con la empresa, en los que se establece la prohibición de revelar cualquier tipo de información que haya adquirido en el desempeño de sus funciones sin el consentimiento expreso de GSI. Adjuntan copia de dicho compromiso de confidencialidad.

Asimismo, informan que los trabajadores de GSI reciben información en materia de protección de datos para el debido cumplimiento de las funciones desempeñadas, información que se facilita a cada uno de los trabajadores y que deben firmar, quedándose cada parte una copia del documento en cuestión. Adjuntan como prueba, además del compromiso de confidencialidad mencionado anteriormente, la circular sobre seguridad de datos personales, la política de uso y control de las tecnologías de la información y las comunicaciones, en la que se incluye la información sobre las restricciones de acceso a las grabaciones del CCTV, y la formación adquirida por el trabajador en cuestión sobre la normativa legal de vigilantes de seguridad.

Por otro lado, señalan el hecho de que los puertos de los equipos del CCTV se encuentran bloqueados, lo que evitaría que las imágenes pudieran ser descargadas en un dispositivo externo, y que la única forma de extraer estas imágenes sería grabando las imágenes mostradas por las pantallas del sistema de videovigilancia a través de un dispositivo externo de grabación de vídeo (teléfono móvil, cámara de vídeo...).

Destacan que, para acceder a la sala de control, donde se encuentran las pantallas de visualización del CCTV, es necesario poseer una tarjeta acreditativa para el control de accesos, tarjeta que posee cada vigilante de seguridad. Además, la mencionada sala de control dispone de una cámara de videovigilancia y la presencia de un vigilante durante las 24 horas del día.

3.- MEDIDAS POSTERIORES A LA BRECHA :

En cuanto a las acciones tomadas con objeto de minimizar los efectos adversos de la difusión del vídeo, cabe mencionar el hecho de que, por parte ITAA, se autodenunció el incidente ante la AEPD con fecha 02/08/2019 y se denunció dicho incidente, también, ante las autoridades policiales el día 07/08/2019. Por su parte, GSI impuso a los trabajadores implicados, tanto en el incidente de agresión como en la grabación del vídeo, una serie de medidas disciplinarias que se dieron a conocer al resto de trabajadores, sin hacer mención del nombre de cada empleado implicado, además de comunicar las medidas adoptadas mediante una nota de prensa.

Por último, destacan que han valorado la posibilidad de restringir el acceso de teléfonos móviles a la sala de control; sin embargo, consideran que esta opción sería inviable al entender que se trata de una herramienta de trabajo imprescindible para los vigilantes de seguridad en el momento de realizar comunicaciones con ITAA.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 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 Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante quiebra 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 que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha confidencialidad por acceso indebido a los datos visualizados por las cámaras de seguridad del centro de control de videovigilancia del ITAA y posteriormente divulgarlos a terceros ajenos a través de la aplicación Whatsapp.

No obstante, también consta que ITAA disponía de medidas técnicas y organizativas para afrontar un incidente como el ahora analizado, lo que ha permitido la detección,

identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante el mismo al objeto de notificar, comunicar y minimizar el impacto e implementar las medidas razonables oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación previamente definido por las figuras implicadas del responsable del tratamiento.

También debe valorarse la adopción de medidas procesales instando la apertura de un procedimiento disciplinario y judicial a través de la oportuna denuncia policial, a los fines de imputación de hechos y reparación del daño causado.

El informe final tras el seguimiento y cierre sobre la brecha y su impacto es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

III

Por lo tanto, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ***INTERCAMBIADOR DE TRANSPORTES AVENIDA DE AMERICA, S.A.U.*** con ***NIF A82059866*** y con domicilio en ***AV. DE AMERICA, NUM 9, PORTAL A, PISO -1, PTA. 1 - 28022 MADRID.***

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 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 de la referida Ley.

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