Expediente Nº: E/05272/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas de oficio por la Agencia Española de Protección de Datos ante la entidad **MERCADONA, S.A.,** y en consideración los siguientes

HECHOS

PRIMERO: Con fecha 04/09/2018 la Directora de la Agencia Española de Protección de Datos (AEPD), al amparo de lo dispuesto en el artículo 11 del Real Decreto-Ley 5/2018, de 27 de julio, de Medidas Urgentes para la Adaptación del Derecho Español a la normativa de la Unión Europea en Materia de Protección de Datos, acordó la práctica de actuaciones de investigación en relación con la noticia difundida en medios de comunicación según la cual los empleados de MERCADONA, S.A., (en lo sucesivo MERCADONA o la investigada) habrían compartido a través de WhastApp imágenes de clientes sospechosos de haber sustraído objetos que fueron facilitadas a esa entidad por la empresa de seguridad privada PROSEGUR ACTIVA ESPAÑA, S.L. (PROSEGUR)

SEGUNDO: La Subdirección General de Inspección de Datos procedió a realizar actuaciones de investigación encaminadas al esclarecimiento de los hechos, teniendo conocimiento de los siguientes extremos que constan en el Informe de Actuaciones de Investigación Previa del que se reproduce el siguiente fragmento:

<<RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Según indican los representantes de Mercadona, con fecha 30 de julio de 2018 fue publicado un artículo en el medio online Merca2.com, bajo el título "Los empleados de Mercadona la lían al compartir imágenes de clientes en WhatsApp" Con carácter previo a su publicación el referido medio contactó con la entidad con el fin de contrastar la información, momento en el que tuvo conocimiento de los hechos e inició los trámites para el su esclarecimiento.
No obstante, de la información a la que tuvo acceso no fue posible determinar la procedencia ni las circunstancias que habían permitido esta situación, informado al medio de comunicación que los hechos descritos en el artículo están prohibidos ya que todos los trabajadores están informados de que no se puede difundir, reproducir o ceder ni hacer un uso personal de las imágenes, fuera de su finalidad que es la seguridad y prevención de los delitos, y que su uso fuera del ámbito de Mercadona está totalmente prohibido", encontrándose esta prohibición recogida en el Convenio Colectivo "como falta muy grave".

Sistemas de videovigilancia de Mercadona.
Mercadona tiene suscrito con Prosegur un contrato para la prestación del servicio de videovigilancia, y dispone de un departamento interno de seguridad (Centro de Atención de Seguridad) para la gestión de estos aspectos.

Dicho Centro de Atención de Seguridad (en adelante, "CAS"), ha establecido un procedimiento interno para la solicitud de las imágenes de videovigilancia que seguidamente se detalla:

1- El coordinador de la tienda solicita al CAS las imágenes, a través de email (es un formato estándar).

a. Puede hacerlo de un periodo concreto (de tal hora a tal hora, del pasillo x), al entender que han faltado productos, y sospecha que se debe a causa de un hurto.

b. Puede solicitar las imágenes de una persona concreta (facilitando los rasgos concretos o descripción de la misma), porque sabe que existe una orden de alejamiento hacia el centro, o bien porque tiene conocimiento que ha cometido un delito.

2- Si el CAS dispone de las imágenes, contestará en el plazo de 48 h, enviando al Coordinador, los fotogramas (no video).

3- Si el CAS, no dispone de las imágenes, o entiende que de ellas no se desprende la comisión de un delito, contestará al centro proporcionando esta información (no están disponibles, no se observan indicios de la comisión de un delito, etc.).

4- Si el CAS envía las imágenes, se realiza siguiendo el método establecido:

a. El acceso a la biblioteca con la finalidad de visualizar las imágenes sólo es posible desde el usuario y con la contraseña del Coordinador.

b. Los fotogramas estarán un máximo de 7 días, después se borran automáticamente.

c. Las imágenes no son descargables, ni imprimibles, e incluyen la marca de agua, el destinatario, y se pixelean las caras no afectadas por los hechos

d. En el email se informa de los criterios que debe seguir el coordinador para el tratamiento de los fotogramas enviados

5- Además el CAS, una vez ha enviado los fotogramas, llama al coordinador de planta, para recordarle los criterios en el tratamiento de las imágenes.

6- Existe un método de trabajo dentro del CAS para las peticiones de imágenes. Incluyéndose en él la advertencia del riesgo de un mal uso de ellas, en el que se hace especial mención a la no difusión de las imágenes a terceros.

7- La finalidad de la petición de imágenes por parte del Coordinador es:

a. Denunciar un posible delito.

b. Prever la comisión de un delito futuro, conociendo a los responsables habituales de la comisión de delitos en los centros de Mercadona podrá proteger mejor a las personas, bienes e instalaciones en ocasiones futuras. Además, evitar posibles incumplimientos de órdenes de alejamiento por parte de los habituales responsables de la comisión del delito.

8- Si tras visualizar las imágenes se comprueba la existencia de un delito se pone en conocimiento de las autoridades dentro del plazo de 72horas.

Medios para evitar la no divulgación de videos.

Los representantes de Mercadona manifiestan que han remitido comunicados a los coordinadores de planta y empleados sobre la prohibición expresa de difundir o utilizar los datos fuera de las funciones corporativas encargadas y su difusión fuera de la empresa.
La medidas de seguridad adoptadas son usuario y contraseña y perfiles de acceso que a juicio de los responsable de la entidad garantizan la protección de la
información y evitan su difusión.

Gestión de brechas e incidentes de seguridad.
Mercadona ha elaborado un procedimiento de gestión de brechas de seguridad Tras tener conocimiento de la noticia publicada realizó las investigaciones oportunas para conocer el alcance de los mismos y hacer las notificaciones oportunas, en caso ser veraces y probados.
Hasta la fecha la entidad no ha tenido conocimiento de las personas afectadas ni de la fuente de la incidencia>>

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos conforme a lo establecido en el apartado 2 del artículo 56, en relación con el apartado 1 f) del artículo 57, ambos del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016 relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (en lo sucesivo, RGPD) y 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)

II

Como se expone en el Antecedente de Hecho segundo de esta resolución con fecha 30/07/2018, a través de un medio de comunicación social, se difundió la noticia de que los empleados de MERCADONA compartían por WhatsApp imágenes de clientes sospechosos de haber efectuado hurtos en los supermercados de la empresa y que tales imágenes procedían de PROSEGUR, con quien la investigada tiene suscrito un contrato para la prestación de servicios de seguridad al amparo de la Ley de Seguridad Ciudadana 5/2014.

La AEPD procedió, a raíz de esa noticia, a efectuar las investigaciones pertinentes para determinar si la investigada había cumplido las obligaciones que le impone la normativa de protección de datos de carácter personal y, en particular, si había adoptado las medidas necesarias para garantizar el principio de "*integridad y confidencialidad"* de los datos.

El RGPD se refiere en su artículo 5 a los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de "*integridad y confidencialidad*" (punto 1 apartado f), que implica que el tratamiento se habrá de

efectuar de manera que "*se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito o contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas*" (el subrayado es de la AEPD).

El mismo precepto (artículo 5.2) hace recaer sobre el responsable del tratamiento de los datos el cumplimiento de los principios que deber regir el tratamiento, así como la prueba de tal cumplimiento, lo que el RGPD denomina "*responsabilidad proactiva*".

En aplicación del principio de "*integridad y confidencialidad"* el artículo 32 del RGPD, bajo la rúbrica "*Seguridad del tratamiento",* dispone*:*

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros." (El subrayado es de la AEPD)

La vulneración por el responsable o el encargado de tratamiento de la obligación impuesta por el artículo 32 del RGPD se encuentra expresamente tipificada como infracción administrativa en el artículo 83.4, apartado a) del RGPD siendo sancionable con multa de un importe máximo de 10.000.0000 de euros o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

III

MERCADONA ha manifestado respecto a los hechos que han determinado la apertura del expediente de investigación, que tiene un compromiso con la intimidad y seguridad de sus clientes; que hechos como los descritos, además de no ser aceptables, están prohibidos por la empresa y que no ha podido determinar, dada la escasa información obtenida, ni la identidad de las personas afectadas, ni la fuente del presunto incumplimiento, ni el origen de la noticia difundida por el medio de comunicación. Añade que, en cumplimiento del RGPD, elaboró un protocolo de gestión de brechas de seguridad del que adjunta copia. El documento lleva fecha de 25/05/2018.

MERCADONA considera que el tratamiento de los datos (la imagen) de los clientes con fines de videovigilancia viene amparada en su interés legítimo en garantizar la seguridad de sus instalaciones, artículo 6, apartado 1.f) del RGPD. Además, en prueba del cumplimiento de la obligación de informar en los términos del artículo 13.1 del RGPD, ha facilitado una fotografía de los carteles informativos disponibles en sus establecimientos que cumple las exigencias del RGPD.

La investigada afirma que al amparo de la Ley de Seguridad Privada tiene suscrito un contrato con PROSEGUR habiendo establecido un Departamento interno de seguridad para, entre otras cuestiones, gestionar la solicitud de imágenes a nivel interno: el Centro de Atención de Seguridad, en adelante CAS.

Afirma también que el CAS tiene fijado un procedimiento para la solicitud de imágenes de videovigilancia que es respetuoso con la normativa de protección de datos personales y cuyos trámites son los siguientes:

1. El coordinador de la tienda solicita a CAS las imágenes a través de un correo electrónico, formato estándar. Señala que puede solicitar imágenes de un periodo de tiempo determinado por entender que faltan productos y sospecha que es debido a un hurto. Y puede también solicitar las imágenes de una persona concreta (facilitando su descripción y rasgos).

2. Si el CAS dispone de las imágenes contesta en un plazo de 48 horas y *envía al coordinador los fotogramas (no video)* (El subrayado es de la AEPD)

3. Si el CAS no dispone de imágenes o entiende que de ellas no se desprende la comisión de un delito informará al centro proporcionando esa información.

4. Si el CAS envía las imágenes al coordinador de la tienda se sigue este protocolo:

   a. "*El acceso a la biblioteca para visualizar las imágenes sólo es posible desde el usuario de entrada del Coordinador a su ordenador (inicio de sesión al sistema), posteriormente el acceso a la carpeta de la Biblioteca, donde se suben los fotogramas, está también limitado exigiendo validación a través de usuario y contraseña del coordinador."*

b. *"Los fotogramas sólo estarán disponibles 7 días y transcurrido ese tiempo se "borran automáticamente".*

c. *"Las imágenes no son descargables, ni imprimibles, e incluyen la marca de agua, el destinatario y se pixelan las caras no afectadas por los hechos .."*. (El subrayado es de la AEPD)

d. En el email se informa al coordinador de los criterios que debe seguir para el tratamiento de los fotogramas enviados. Se incluye la siguiente cláusula:

<<Las imágenes e información contenida en el presente correo es confidencial y su finalidad es, exclusivamente, la gestión de los incidentes de seguridad, tanto física como en relación con los bienes e inmuebles de Mercadona conforme a la normativa vigentes en materia de protección de datos y seguridad. Queda terminantemente prohibida su captación por dispositivos móviles, grabación, difusión o reproducción fuera de los sistemas corporativos y de las pautas fijadas por el área de seguridad de Mercadona.

El presente correo se remite como contestación a la solicitud realizada por …, con las exclusivas finalidades reseñadas. El destinatario del presente correo se responsabiliza de los posibles incumplimientos de los aspectos reseñados, así como de la normativa vigente>>

e. Que el CAS, una vez enviados los fotogramas al coordinador de la tienda/planta le llama por teléfono para recodarle los criterios a seguir en el tratamiento de las imágenes haciendo mención a la no difusión de las imágenes a terceros.

De lo manifestado por MERCADONA se evidencia que únicamente el coordinador de la tienda/planta está habilitado, previa acreditación a través de su usuario y contraseña, para acceder a la Biblioteca y visualizar los fotogramas que le envíe el CAS relativos a los presuntos delincuentes.

Hay que añadir que, según lo declarado por la investigada, las imágenes que se cuelgan en la Biblioteca y a las que accede el coordinador de tienda están disponibles 7 días desde el momento en que se envía la contestación, lo que resulta acorde con la previsión del artículo 6 de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras -en adelante la Instrucción-. La citada Instrucción está vigente en todo aquello que no se oponga al presente RGPD y a la LOPDGG y dispone que los datos serán cancelados en el plazo de un mes desde su captación.

Hemos de subrayar que, según lo expuesto por la entidad a través del escrito remitido por su DPO, las medidas de seguridad adoptadas por MERCADONA comprenden también el uso que el coordinador de tienda puede hacer de los

fotogramas a los que accede.

En este sentido, a tenor de lo manifestado por la investigada, las imágenes o fotogramas que el CAS facilita al coordinador de tienda no son descargables ni imprimibles. Por otra parte, el Convenio Colectivo de Mercadona publicado en el BOE el 30/01/2014 prohíbe la extracción de información de la empresa a cualquier dispositivo de almacenamiento de uso privado de la persona siendo esta conducta constitutiva de infracción muy grave. El artículo 33 del Convenio, "*Régimen sancionador*", detalla las conductas que constituyen infracciones muy graves, graves y leves y en su apartado c, infracciones muy graves, punto 3, describe la obligación precitada.

Con fines de prueba ha remitido a la AEPD copia de dos correos electrónicos enviados por los coordinadores de tienda al CAS en los que solicitan que les faciliten imágenes referentes a una zona específica de la tienda, a una cámara determinada y, a un intervalo horario en uno de los casos y, en otro, relativas a la persona que describen.

Es digno de mención, no obstante, que el tenor de los correos electrónicos revela algunas diferencias entre el "modus operandi" no coincide plenamente con lo declarado a la AEPD en la respuesta al requerimiento informativo. Así, en uno de los correos electrónicos facilitados por la investigada el coordinador de tienda, después de explicar al CAS a qué zona de la tienda se refieren las imágenes que solicita y el motivo de su petición, añade: "*Necesitaría ver las imágenes para detectar el hurto y mostrar a la plantilla para poder denunciar los posibles hurtos".* (El subrayado es de la AEPD)

No obstante, no cabe concluir de lo anterior que, tal y como sostuvo el medio de comunicación que publicó la noticia que ha motivado que la AEPD llevara a cabo actuaciones de investigación para depurar posibles responsabilidades por infracción de la normativa de protección de datos, los empleados de la investigada se hubieran intercambiado a través de WhatsApp imágenes de presuntos delincuentes. Las imágenes que el CAS facilita a los encargados de tienda no son descargables a lo que se añade que constituye una infracción muy grave el descargarse en los dispositivos privados, como lo son los teléfonos móviles de los empleados, cualquier información obtenida de la empresa. Con toda claridad el Convenio Colectivo de Mercadona prohíbe expresamente la extracción de información de la empresa a cualquier dispositivo de almacenamiento de uso privado de los empleados siendo constitutiva de una infracción muy grave la vulneración de esta obligación.

Añadir a lo expuesto que la investigada remite la copia del email enviado a los coordinadores el 30/07/2018, recordándoles la prohibición expresa de difundir o utilizar los datos -toda la información relativa a sus clientes- fuera de las funciones corporativas encargadas y su difusión fuera de la empresa. Insiste también en la prohibición de tratar y difundir los datos en sistemas no corporativos o por medios no autorizados por MERCADONA.

Así las cosas, habida cuenta de que, a la luz de la exposición precedente, no existen indicios razonables de que la investigada hubiera incumplido las obligaciones que le impone el RGPD en cumplimiento del principio de integridad y confidencialidad y de que las investigaciones efectuadas no han permitido obtener indicio razonable alguno de la existencia de una brecha de seguridad en el tratamiento que hace MERCADONA de los datos de sus clientes, procede acordar el archivo de las actuaciones de investigación realizadas.

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **MERCADONA, S.A., con** NIF ***A-46103834.***

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 y, de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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