824-150719

Procedimiento Nº PS/00336/2018

RESOLUCIÓN: R/00423/2019

En el procedimiento sancionador PS/00336/2018, instruido por la Agencia Española de Protección de Datos a la entidad **CECOSA HIPERMERCADOS, S.L.,** y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha de 25/04/2018, la directora de la AEPD acuerda iniciar las presentes actuaciones de investigación en relación con la publicación ese mismo día, en diferentes medios de comunicación, de imágenes procedentes de las grabaciones registradas por el sistema de videovigilancia instalado en un establecimiento comercial de la cadena de supermercados EROSKI correspondientes a hechos acaecidos el 4/05/2011.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se realizan las siguientes:

1) El periódico digital "*El Español*" informa en *(***URL.1)* que el supermercado EROSKI en el que tuvieron lugar los hechos investigados cerró meses después de ocurridos estos, traspasándose el establecimiento a otra cadena para, finalmente, ser vendido a otro operador que es el que lo gestiona actualmente.

2) Asimismo, varios medios digitales y de prensa identifican a CASTELLANA SEGURIDAD, S.A.,(CASESA) como la empresa que se encargaba de la seguridad del establecimiento en los momentos de producirse el incidente. Se comprueba, en su página web, con fecha 26/02/2018 que se informa de la inscripción en el Registro Mercantil de Madrid, de la escritura de fusión de CASTELLANA SEGURIDAD, S.A.U. por su socio único OMBUDS COMPAÑÍA DE SEGURIDAD, S.A., (OMBUDS).

TERCERO**:** Con fecha 27/04/2018 se realiza una inspección en las oficinas de la sede de OMBUDS COMPAÑÍA DE SEGURIDAD, S.A., empresa que, tal y como se ha indicado anteriormente y confirma el director del Servicio Jurídico, realizó sobre la sociedad CASESA una operación societaria de fusión por absorción, quedando extinguida la personalidad jurídica de esta última desde finales de 2017 y sucediéndola universalmente OMBUDS en todos sus derechos y obligaciones.

a) Durante la inspección, manifiesta que tanto el vigilante que aparece en el video publicado en los medios de comunicación como la persona que desempeñaba el puesto de Inspector/Coordinador de zona, ***A.A.A.*** (A.A.A.) y que, con anterioridad a los hechos, había sido Jefe de Seguridad en el referido establecimiento comercial, siguen formando parte de la plantilla de OMBUDS tras la operación de fusión por absorción, y que conocen en detalle el funcionamiento del centro en lo relativo a la seguridad.

Se aporta además copia del cuadrante de servicio del mes de mayo de 2011 en el que figura la relación de vigilantes propuestos para cubrir el servicio de vigilancia en el establecimiento comercial indicando que se va a intentar localizar los partes o informes diarios

de servicio correspondientes a dicho mes y en el que estarían reflejadas las incidencias ocurridas, documento que queda requerido en la inspección realizada. No obstante, refiere que no les consta que los agentes de Policía que se personaron en el establecimiento comercial solicitaran copia de las grabaciones en relación con la incidencia acaecida.

Aclara que, según la "*información facilitada por el Sr,* A.A.A.*, los posibles accesos al videograbador del establecimiento comercial sólo podían realizarse desde el despacho del Gerente de Eroski, que era la única persona habilitada para realizar tratamientos en modo local*". Además, la sociedad titular del establecimiento comercial tenía suscritos dos contratos, de instalación y mantenimiento de las cámaras bien con la empresa INGECOM o bien con EQUINSA, desconociéndose con certeza cuál de ellas era la contratada y otro de conexión nocturna a central receptora de alarmas (CRA) con SABICO.

b) Manifiesta que el servicio de seguridad que prestaba CASESA en el establecimiento comercial era de mera vigilancia, sin acceso a los sistemas de videovigilancia, no contando la empresa con habilitación para la instalación ni el mantenimiento de los dispositivos de seguridad, indicando que ello figura en el contrato de servicio de seguridad, de 14/02/2011 que aporta (doc. 3), añadiendo el pliego jurídico y otro técnico. Indica que CASESA figura habilitada únicamente para las actividades de *"vigilancia; protección, de bienes; establecimientos; espectáculos, certámenes o convenciones"* y con ámbito de actuación nacional.

El contrato de 14/02/2011 "*de arrendamiento servicios seguridad vigilancia*" se suscribe entre CECOSA SUPERMERCADOS SL y CASESA. Figura que CECOSA HIPERMERCADOS SL, cadena de distribución de productos de alimentación explota una amplia red de establecimientos comerciales, y requiere contratar la prestación de servicios de vigilancia, indicándose que la adjudicación ha sido precedida de unas bases y que CASESA participó en el concurso y ha sido adjudicataria y suscriben ese contrato marco " *de prestación de servicios*". Se destaca del mismo:

-CECOSA, dedicada a la distribución de productos de alimentación y otros explota una amplia red de establecimientos comerciales y dispone de almacenes, oficinas, aparcamientos etc. para llevar a cabo la actividad que le es propia. A tal efecto requiere contratar la prestación de servicios de diverso tipo entre los cuales se encuentran los que son propios de los trabajos o servicios de vigilancia, razón por la que ha realizado un concurso para su adjudicación.

-El servicio contratado es de "*vigilancia*" y su duración hasta 31/0172013, entrando en vigor el 1/03/2011.

- El servicio se prestará en HIPERMERCADOS DEL GRUPO EROSKI.

-Se indica en la estipulación adicional primera que el orden de prevalencia en caso de discrepancia seria el del contrato marco, pliego de condiciones técnicas, ANEXO I con los servicios a prestar por el contratista, normas generales

Por tanto, no se concreta centro alguno, siendo un contrato marco. En la estipulación DECIMOQUINTA del contrato de 14/02/2011, relativa a la confidencialidad, donde se regula las obligaciones del contratista derivadas del tratamiento de los datos de carácter personal a los que pudiera tener acceso en el cumplimiento de la prestación. Según consta en el contrato, reforzando el carácter genérico del mismo y sin especificar las necesidades particulares de cada establecimiento objeto del servicio, *"en aquellos casos en que el Contratista, directamente o a través de sus empleados, pudiera tener acceso a Datos de Carácter Personal, en general entendidos como los definidos en la LOPD , entre los que se encuentran los relativos a la videovigilancia y el control de acceso físico, se obliga a", no*

comunicarlos ni cederlos y a mantener el carácter confidencial de los mismos, así como a adoptar y respetar las medidas organizativas, técnicas y de seguridad que la Propiedad estime necesarias. Respecto a esas medidas de seguridad, el contrato consigna que *"El Contratista y sus empleados tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. La Propiedad establecerá los mecanismos para evitar que el Contratista pueda acceder a recursos con derechos distintos a los autorizados, por ello el Contratista se encargará de que exista una relación actualizada de usuarios y perfiles con acceso autorizado al Sistema de Videovigilancia que capta y almacena las imágenes, que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información".*

En la cláusula 15.3 establece que el contratista se compromete a adoptar las medidas de seguridad que el titular estime necesarias de acuerdo con lo establecido en la LOPD para garantizar la confidencialidad y seguridad de los datos, siendo el nivel de seguridad de los datos derivados de la prestación de servicios, el básico, Se indica que el contratista y sus empleados tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. Y que "*el contratista se encargara de que exista una relación actualizada de usuarios y perfiles con accesos autorizados al sistema de videovigilancia que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información*". "*Exclusivamente la propiedad en coordinación con el contratista o viceversa, podrá conceder, alterar o anular el acceso autorizado sobre los sistemas de videovigilancia*." "*Se prevé también que si los soportes y documentos que contengan datos de carácter personal, así como las grabaciones en disco o cinta salieran de los locales donde se lleva a cabo la prestación de servicios, requerirá autorización por parte de la propiedad*" y que "*El contratista deberá notificar a la propiedad las incidencias que afecten a los datos de carácter temporal. Asimismo, establecerá un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso detectado*…". Se deduce que cualquier extracción de las grabaciones del sistema de videovigilancia a un soporte, de acuerdo al protocolo de tratamiento de la imagen definido por el propio GRUPO EROSKI para todos sus puntos de venta, debería haber sido realizado o, en su caso, haber estado autorizado o supervisado por el personal definido en el protocolo y haber contado, de acuerdo con el contrato suscrito y el propio protocolo, con las medidas de seguridad apropiadas para garantizar que sólo pudiera realizarse bajo la autorización del Responsable del Fichero.

c) Indica que en el lugar donde se produjeron los hechos existe ahora un supermercado CARREFOUR en el que ellos tienen un contrato de vigilancia por medio de personal, sin acceso a los sistemas de videovigilancia. Adjuntan documento 5

CUARTO: En ampliación a la información ya recabada y la pendiente de facilitar por OMBUDS COMPAÑÍA DE SEGURIDAD, S.A. a raíz de la inspección realizada el 27/04/2018, se solicitó el 4/05/2018 la siguiente información en relación con el sistema de videovigilancia que estaba instalado en el establecimiento comercial del GRUPO EROSKI arriba referido:

1. Documentación completa de la oferta presentada por CASESA**.,** en el marco del concurso realizado por el GRUPO EROSKI en diciembre de 2010 para la adjudicación del servicio de vigilancia de negocios del grupo empresarial. En la documentación presentada deberá figurar:

-El Plan Operativo relativo al desarrollo del servicio al que se hace referencia en el apartado 9.- PLAN OPERATIVO. - del Pliego de Condiciones Técnicas y que deberá

incluir, según refiere ese punto, copia del manual de procedimientos en el que se especifique las funciones a realizar para cada puesto de trabajo.

-Posibles sugerencias de mejoras propuestas en la prestación del servicio ofertado.

Con fecha 16/05/2018 acompañan documentos 4 a 9 donde consta la oferta presentada por CASESA a EROSKI que incluye índice, plan operativo, formación, mejoras, plan de selección y oferta económica con detalle de costes.

El Pliego de Condiciones Técnicas exigía, en su apartado *9.- PLAN OPERATIVO*, la presentación, por parte de las empresas licitadoras, de un plan operativo relativo al desarrollo del servicio basado en los datos incluidos dentro de los pliegos de cláusulas administrativas y técnicas que debía describir, entre otras cosas, las funciones a realizar para cada puesto de trabajo. En la oferta presentada por CASESA, respecto a las funciones identificadas para el personal adscrito al centro de control, se define el *"control mediante el CCTV de todas las zonas de la instalación"* y el *"seguimiento mediante el CCTV de las personas sospechosas"*, sin ofertarse expresamente el acceso y gestión de las grabaciones de seguridad realizadas por el sistema de videovigilancia por parte de CASESA.

-Sobre el punto 2.8 de la visita de Inspección indican que "*no ha podido localizar los partes de servicios diarios de mayo 2011*"

2. Documentación pendiente a la ya facilitada, según la estipulación adicional "*PRIMERA.- OBJETO*", que completa el contrato de arrendamiento de servicios de seguridad vigilancia suscrito entre CECOSA y CASESA firmado el 14/02/2011, y entre la que deberá estar incluido el documento identificado como "*Anexo I con los servicios a prestar por el Contratista*".

-Aportan en documento 1, anexo de pliego de prescripciones técnicas, pliego jurídico y normas generales, que completa el punto 2.6 del acta de Inspección apareciendo firmado.

3. Si CASESA firmó antes de su absorción por OMBUDS algún contrato con EROSKI SOCIEDAD COOPERATIVA que se mantiene vigente en la actualidad, facilitar copia firmada y completa del mismo.

Señala OMBUDS que CASESA cesó de prestar servicios para EROSKI en 2014 tras verse rechazada su oferta, se acredita en documento 13, debiendo considerar que en supermercado donde suceden los hechos cerró en 2011.

4. Confirmar, de acuerdo con lo indicado en el apartado 1 de la estipulación adicional DECIMO QUINTA del contrato, relativa a los datos de carácter personal, si el contratista, directamente o a través de sus empleados pudo tener acceso a datos de carácter personal, y en concreto a datos relativos a la videovigilancia. Describir en qué consistía dicho acceso y cómo se producía.

Reitera que no consta en sus archivos, que CASESA o sus empleados accedieran a datos para la prestación del servicio, incluyendo la videovigilancia.

Aporta como documento 3 y 4 sin que hayan sido solicitadas, transcripción de las declaraciones que dice se han prestado ante la Unidad de Seguridad Ciudadana por parte de Sr. A.A.A., y el vigilante que se ve en las imágenes publicadas en los medios.

En dichas declaraciones, el vigilante de seguridad manifiesta que, en el día de los hechos, prestando servicio en el centro de control del hipermercado EROSKI del Centro Comercial Madrid Sur, *"pudo observar por los monitores como una mujer rubia, vestida de azul, probaba productos en la sección de perfumería, y como portaba un bolso, en el cual introdujo, hasta en dos ocasiones productos de cosmética." Continua en su declaración de los hechos que, esperando a la mujer en línea de cajas y solicitándole que le acompañase al cuarto de intervenciones al ver que no abonaba los cosméticos introducidos en el bolso, le preguntó que "si portaba algún producto que no hubiera abonado, respondiéndole la mujer que no"*. "*Tras realizar varias comprobaciones y confirmar que portaba los envases de crema, el vigilante de seguridad avisó al jefe de equipo y que identifica como la otra persona que aparece en el video publicado, para que cuantificara los importes. Habiéndole solicitado a la mujer que abonara los productos", "en primer momento se negó a pagarlos, alegando que no los había sustraído, ante la negativa al abono, el jefe de equipo decidió llamar a la Policía Nacional"*, personándose dos agentes vestidos de paisano en el establecimiento. Transcurridos unos cuarenta y cinco minutos, se resuelve el incidente y abandonando la mujer el Centro Comercial por una salida de emergencia. Completa sus manifestaciones en aclaración al servicio prestado diciendo que él sólo tenía acceso al visionado de las imágenes en tiempo real y no a las imágenes grabadas con anterioridad, aclarando que en el tiempo que estuvo trabajando en el hipermercado, ni las Fuerzas y Cuerpos de Seguridad ni otros solicitantes le pidieron nunca grabaciones de imágenes, desconociendo quién era la persona encargada de facilitarlas en caso de ser requeridas.

Por su parte, el trabajador de OMBUDS que prestaba servicios como Inspector de Servicios de zona para CASESA en el momento de los hechos, Sr. A.A.A., manifiesta en su declaración que la persona autorizada para tratar las imágenes grabadas por el sistema de videovigilancia *"era el Director del Centro y Gerente (….) que tenía en su despacho el ordenador con el programa para extraer las imágenes*", aclarando que *"en caso de urgencia, también podían extraer las imágenes personal del centro, como la Jefa de personal (…) y el encargado de Bazar (…)."* Respecto al protocolo seguido para recuperar las imágenes y aportarlas a la Policía para efectuar la correspondiente denuncia, refiere que *"esta lo solicitaba a través de los vigilantes de seguridad, del inspector de servicios, del director del supermercado o en su defecto de la persona que quedase al cargo. El despacho en el que se encontraba el ordenador para extraer las imágenes se encontraba permanentemente cerrado con llave, teniendo acceso al mismo el director del centro y la responsable de recursos humanos. Una vez obtenidas las imágenes, que se grababan en un CD, eran entregadas por quien las había obtenido al servicio de seguridad para que estos le dieran el trámite oportuno".* Asimismo, aclara que "*no tiene conocimiento de que las imágenes del suceso publicado en los medios de comunicación fuesen solicitadas al servicio de seguridad y que nadie de dicho servicio pudo recuperar dichas imágenes*" *"ya que para acceder al despacho del ordenador desde donde se gestiona el software había que disponer de la llave del mismo, teniendo acceso sólo a ella, el director del centro y la jefa de recursos humanos."*

5. Aclarar el punto 3 de la estipulación adicional DECIMO QUINTA del contrato, relativa a los "*datos de carácter personal*" donde se indica que "el *Contratista se encargará de que exista una relación actualizada de usuarios y perfiles con accesos autorizados al Sistema de*

Videovigilancia que capta y almacena las imágenes". Descripción detallada de los perfiles facilitados a la Propiedad, especificando sus funciones, capacidades y alcance, así como la relación de usuarios asignados a los perfiles definidos.

Reitera que no existía acceso por parte de los vigilantes de CASESA y que la cláusula en su elaboración responde a un modelo genérico, que "*el acceso solo se daba por personal del propio EROSKI*", y "*los vigilantes se limitaban al visionado en tiempo real*".

6. Confirmar si, durante el período de 30 días posteriores al 4/05/2011, CASESA directamente o a través de sus empleados que prestaban servicio en el establecimiento comercial EROSKI VALLECAS, pudo tener acceso a las grabaciones publicadas objeto de esta investigación y facilitar copia de estas a petición de un tercero. En caso afirmativo, identificar a las partes implicadas en la comunicación de las grabaciones.

Reitera que sus empleados no tenían acceso.

7. Facilitar un croquis o plano de situación aproximado de las instalaciones del establecimiento EROSKI VALLECAS donde se identifique claramente donde se encontraba el cuarto de intervención de seguridad donde tuvieron lugar los hechos cuyas imágenes han sido publicadas, así como las dependencias donde se situaban los monitores de videovigilancia y el sistema de grabación de las imágenes registradas por las cámaras, especificando a cuáles de esos espacios tenía acceso autorizado el personal de CASESA.

Acompañan el citado croquis en documento 14.

8. Aportar copia del documento identificado como ANEXO III: PROTOCOLO DE ACTUACIÓN que forma parte del contrato de servicios de vigilancia suscrito entre el GRUPO CARREFOUR y CASESA con fecha 8/03/2016.

Manifiesta que no consta dicho protocolo como anexo III al contrato ni su mención, pero si figuran procedimientos de actuación dentro del plan operativo y aporta un documento 5 con el logo GRUPO EROSKI, plan operativo.

En correo electrónico de 17/05/2018, registro de entrada 21, añaden el protocolo actuación anexo III contrato OMBUDS-CARREFOUR 2016.

QUINTO: A OMDUDS también se le requirió el 30/05/2018:

-Copia del documento identificado como "*Manual de Órdenes de Puesto*" en la oferta presentada por CASESA, en el marco del concurso realizado por el GRUPO EROSKI en Diciembre de 2010 para la adjudicación del servicio de vigilancia de negocios del grupo empresarial, así como de todos aquellos manuales de procedimientos de actuación en materia de videovigilancia y protección de datos, entre ellos "*Procedimiento para el centro de control de seguridad",* "*Procedimiento para la protección de la información*" y "*Procedimiento de control de acceso de personas a las instalaciones*".

OMBUDS COMPAÑÍA DE SEGURIDAD, S.A. manifiesta el 20/06/2018 que no ha sido posible localizar en los archivos la documentación requerida ni el personal de *CASESA* incorporado a *OMBUDS* ha podido dar razón de la misma.

Sí que se aporta copia del *"Manual Operativo del Servicio de Seguridad de CECOSA* HIPERMERCADOS,S.L. EROSKI HIPER y EROSKI C.P" para los servicios de seguridad que actualmente OMBUDS COMPAÑÍA DE SEGURIDAD, S.A. presta en distintos establecimientos comerciales del GRUPO EROSKI y en el que se recogen los cometidos, las órdenes y los procedimientos operativos que deben seguir los vigilantes de seguridad en el servicio prestado; es decir, qué deben hacer y cómo deben hacerlo.

Profundizando en el perfil y las características del Puesto de Vigilancia, de los siete cometidos recogidos relativos a "*Control de Accesos*", "*Realización de Rondas*", "*Actuación ante emergencias y alarmas*", "*Actuación ante una amenaza telefónica de bomba*", "*Actuación ante alborotos*", "*Actuación ante la detección de un posible paquete o coche bomba*" y "*Colaboración con otros servicios de seguridad*", los cuales vienen definidos con extremo nivel de detalle, en el Cometido nº 3 relativo a la *"Actuación ante Emergencias y Alarmas"*, en el Procedimiento Operativo nº 2 en relación con la actuación *"ANTE ROBO, HURTO o ROTURAS"* se recoge textualmente que *"A fin de evitar situaciones posteriores complicadas (como denuncias del cliente, etc.) el vigilante debe intervenir tras llegar a estar completamente seguro. Para ello, estará en contacto con el 'Centro del C.C.T.V.' averiguando si ha quedado constancia de los hechos en la grabación del Circuito Cerrado de Televisión"* y que *"el vigilante, en su intervención ante un robo o hurto debe tener en cuenta lo siguiente: (…) Informará al cliente de que, ante la evidencias disponibles, debe abonar los productos o, en su defecto, devolverlos."* lo que parece poner de manifiesto la posibilidad de acceder, por parte del personal de la empresa de seguridad, a las grabaciones de eventos registrados desde la sala de CCTV a los efectos de comprobar la posible sustracción de productos.

No obstante, dicho manual identifica el perfil de "*Responsable de Seguridad*", como personal encargado de la dirección, supervisión y prestación de la seguridad en CECOSA HIPERMERCADOS, S.L., EROSKI HIPER y EROSKI C.P. en la figura del Gerente, haciendo repetidas referencias a las consultas, instrucciones e indicaciones dadas por el Responsable de Seguridad del establecimiento comercial en el marco de los distintos procedimientos operativos definidos en el *Manual Operativo del Servicio de Seguridad* que debían ser seguidas por los vigilantes que prestan el servicio, en clara sintonía con lo estipulado tanto en el contrato de prestación de servicios como en el protocolo de tratamiento de la imagen y el extracto del manual de seguridad ya referenciados en lo que respecta a la revisión de las medidas de seguridad así como a la supervisión y autorización de los accesos a los sistemas de videovigilancia y la salida de soportes por parte de la Propiedad.

- Indicar si OMBUDS COMPAÑÍA DE SEGURIDAD, S.A. mantiene en la actualidad algún contrato para la prestación de servicios de seguridad con CECOSA HIPERMERCADOS, S.L., facilitando, en caso afirmativo, copia firmada y completa del mismo.

Manifiesta que tienen vigente contrato con CECOSA HIPERMERCADOS S.L. para la prestación de servicios de seguridad. Aporta copia del contrato de 26/04/2014. Figura la cláusula DECIMOQUINTA, relativa a la confidencialidad, que es copia exacta de la cláusula arriba analizada que regulaba este aspecto del servicio en el contrato suscrito entre CECOSA HIPERMERCADOS, S.L. y CASESA en febrero de 2011, con la única salvedad de que en lugar de "a la Propiedad" hace referencia "al Cliente" y el contrato actualmente

vigente amplía su alcance a más empresas del grupo empresarial y entre las que se encuentra CECOSA HIPERMERCADOS, S.L., en lugar de circunscribirse a esta última.

Por su parte, el Pliego de Condiciones Técnicas exigía, en su apartado *9 .- PLAN OPERATIVO*, la presentación, por parte de las empresas licitadoras, de un plan operativo relativo al desarrollo del servicio y basado en los datos incluidos dentro de los pliegos de cláusulas administrativas y técnicas que debía describir, entre otras cosas, las funciones a realizar para cada puesto de trabajo. En la oferta presentada por CASESA, respecto a las funciones identificadas para el personal adscrito al centro de control, se define el *"control mediante el CCTV de todas las zonas de la instalación"* y el *"seguimiento mediante el CCTV de las personas sospechosas"*, sin ofertarse expresamente el acceso y gestión de las grabaciones de seguridad realizadas por el sistema de videovigilancia.

SEXTO: EROSKI SOCIEDAD COOPERATIVA, (EROSKI SC) empresa matriz del grupo que da nombre a la marca comercial del hipermercado en el que tuvieron lugar los hechos el 4/05/2011, en Avenida Pablo Neruda 91–97, Madrid, conocido como EROSKI VALLECAS remite escritos de 14, 15 y 17/05/2018 en respuesta a la petición de 26/04/2018 sobre la cuestión relacionada con la reproducción de una grabación de un sistema de videovigilancia publicada en diferentes medios.

Se le solicitó:

a) Identificación del responsable del sistema de videovigilancia

Manifiesta que la sociedad titular del establecimiento comercial cuando tuvieron lugar los hechos era CECOSA HIPERMERCADOS, S.L., (CECOSA) que pertenece al grupo empresarial. Manifiestan que las respuestas proporcionadas, lo han sido, como empresa corporativa y por economía y eficacia procesal, remitiendo a la empresa titular del hipermercado para que facilite toda aquella información que afecte a datos personales.

b) Identificación de la empresa encargada de la seguridad del mencionado establecimiento comercial en el momento en que tuvo lugar la captación de las imágenes, 4/05/2011 facilitando copia del contrato de prestación de servicios suscrito, así como la identificación de todos los vigilantes de seguridad, junto con su credencial, que prestaban servicio en el marco de dicho contrato en el momento de los hechos.

Responde que era CASESA la encargada de prestar los servicios, con acceso a las grabaciones dentro del centro, aportando copia del contrato "*marco*" de 14/02/2011 suscrito con CECOSA (ANEXO 2).

En cuanto a los vigilantes de seguridad, EROSKI manifiesta que "*no podemos aportar datos de los vigilantes de seguridad, ni credencial alguna*".

c) Información sobre la identidad de la empresa que realizó la instalación del sistema de videovigilancia que estaba operativo en el momento de realizarse las grabaciones objeto de investigación. En caso de haberse contratado un servicio de mantenimiento del sistema, describir el alcance de este aportando copia del correspondiente contrato.

La empresa encargada de la instalación del sistema de videovigilancia se denomina EKINTZA, ya extinguida sin constar, según manifiestan, copia del contrato. Se incorpora diligencia del Boletín Oficial del Registro Mercantil de 17/06/2014 con la

anotación d extinción. Aportan "*extracto ANEXO 3 VHP Vallecas-Datos policía contratos*" consistente en un listado de EKINTZA en el que figuran, según manifiesta los números de contratos de instalación y mantenimiento de sistemas con EKINTZA entregados a la policía números 149/10 y 153/10. Añaden que no consta ni factura ni presupuesto de 2011.

Una empresa denominada SABICO era la encargada de la Central Receptora de Alarmas (CRA) con capacidad de acceso remoto a las grabaciones del sistema y para la que, en el momento de dar respuesta a los requerimientos realizados por esta Agencia con fechas 26/04 y 22/05 tampoco aportan copia del contrato suscrito.

d) Causas que motivaron la instalación de las citadas cámaras,

Responde que garantizar la seguridad de bienes y personas, así como servir de mecanismo de control para el cumplimiento de las obligaciones laborales.

e) Descripción de las características técnicas del sistema que estaba instalado, número de cámaras, croquis, tipo de cámara ubicada en el cuarto de seguridad cuyas grabaciones han sido publicadas y otras cuestiones relacionadas

Indica que como el centro no era de su titularidad pues se vendió a finales de 2011, "*ni la empresa proveedora existe según se ha averiguado, no podemos contestar a esta cuestión*".

f) Detalle de las medidas de seguridad implantadas en el establecimiento EROSKI VALLECAS en el momento en que tuvieron lugar los hechos investigados en lo que se refiere a:

Protocolo específico en materia de videovigilancia y/o seguridad, aportando copia de este.

Aportan ANEXO 4 "*tratamiento imágenes de videovigilancia, Grupo Eroski* " de marzo 2009 que determina las bases para el tratamiento de imágenes a través de videocámaras. Se indica:

-EROSKI SC es la sociedad matriz del GRUPO y en cumplimiento de las obligaciones asumidas como tal, presta servicios generales, gestión de recursos humanos, comerciales, jurídicos, de administración e informáticos a las SOCIEDADES del Grupo. EROSKI SC "*accederá a determinada información, necesaria para el cumplimiento de las obligaciones asumidas y en consecuencia, se convierte en encargada del tratamiento para toda ellas*."

Se contiene un cuadro de "*fichero videovigilancia*" dividido en "*seguridad privada*" y "*control laboral*" figurando los responsables y los encargados. Como encargados en todos los casos de videovigilancia, figura "*empresas de seguridad*". Consta también una entidad denominada "*CECOSA SUPERMERCADOS SL*", de forma diferenciada de "CECOSA HIPERMERCADOS SL" como responsables en seguridad privada.

Se indica también que "*Para el entono de seguridad privada, EQUIPAFASA será encargadas del tratamiento de CECOSA HIPERMERCADOS, por ser ésta última la Sociedad responsable de ese tratamiento, como norma general, en los hipermercados y algo similar sucede con CENCO, SUPERA, UDAMA Y DAGESA, ya que CECOSA*

SUPERMERCADOS es la responsable del fichero de videovigilancia para el entorno de Supermercados". "*Todas estas sociedades disponen de un acuerdo que regula el acceso a los datos de carácter personal*". Indica que: "*Cuando se capten y/o registren imágenes y la empresa de seguridad contratada utilice las videocámaras y/o acceda a las imágenes por medio de su personal, la empresa de seguridad se convertirá en encargada del tratamiento según la LOPD y así deberá constar en el contrato que será obligatorio suscribir con el proveedor*." También se anota que "*Todo responsable de fichero que trata imagen bien por seguridad bien para el control de obligaciones laborales, tiene debidamente inscrito en el Registro General los ficheros*"

En el punto 22.2 "*REQUISITOS PARA EL TRATAMIENTO FINALIDAD SEGURIDAD PRIVADA*" se indica en el punto 2.2.2.1 punto 5: "*Cuando se capten y/o registren imágenes con fines de seguridad privada y la empresa de seguridad contratada utilice las videocámaras y/o acceda a las imágenes por medio de su personal, la empresa de seguridad se convertirá en encargada del tratamiento según la LOPD y así deberá constar en el contrato que será obligatorio suscribir con el proveedor".*

Punto 6. *Las imágenes se conservarán como máximo un mes, salvo si surgiera una incidencia que obligara a su conservación por un periodo superior. 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 obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica.*

7. Estos ficheros o tratamiento de datos adoptan las medidas de seguridad calificadas de nivel básico. Las medidas tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa se pudieran adoptar.

a. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a las imágenes están definidas y conocen las normas de seguridad que afectan al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

b. La notificación y gestión de las incidencias que ponga en peligro la integridad, disponibilidad y confidencialidad de las imágenes quedará debidamente documentada y registrada.

c. Existe una relación tasada y limitada de usuarios/ personal con acceso autorizado a ese conjunto de datos con su correspondiente identificación y autenticación. Según la actuación podría ser necesario que accediera uno, varios o todos los usuarios implicados:

i. Usuarios del Área de Garantía Patrimonial Corporativa.
ii. Responsables de seguridad física.
iii.Responsable jurídico LOPD.
iv. Gerentes y/o Jefes de Tienda
v. Responsable del Área Jurídico Laboral.

d. Se realizarán copia de respaldo, como mínimo, semanal, salvo que en dicho período no se hubiera producido ninguna actualización de los datos o el plazo de almacenamiento de las imágenes sea inferior debido al sistema de almacenamiento.

e. Las redes de comunicaciones a través de las que se pude llegara a acceder a las imágenes, garantizan un nivel de seguridad equivalente al correspondiente a los accesos en modo local.
Los soportes, que así lo permitan y que pudieran llegar a contener las imágenes (DVD, disco duro o USBs) identificarán el tipo de información que contienen y serán inventariados. Sólo serán accesibles por el personal autorizado.

g. El responsable de fichero autoriza, exclusivamente, al personal / usuarios descritos en este apartado la salida de esos soportes y obliga, en su traslada, a adoptar medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información.

h. Cuando ese soporte deje de ser necesario y vaya a desecharse, deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

2.2.3 FASE (3)_ POSIBLES INCIDENCIAS
2.2.3.1 (3.1 .A) ENTORNO SEGURIDAD PRIVADA CONTRA BIENES Y PERSONAS
Cuando se detecte una incidencia que atente contra las personas o los bienes (robos, hurtos, estafas, etc.) intervendrán los diferentes responsables, dependido del entorno.

Se acudirá a las Fuerzas y Cuerpos de seguridad con el objeto de poder denunciarlo y así poder mantener las imágenes, que nos pueda servir como medio de prueba, incluso por más tiempo del máximo permitido.

Si fuera necesario, se recurrirá a la empresa de seguridad para recuperar las imágenes que recojan el incidente.

Si la Autoridad Competente, en cada caso, o las Fuerzas y Cuerpos de Seguridad solicitaran visionar las imágenes, se les permitirá, previo requerimiento oficial o denuncia.

En todo momento, el Gerente/Jefe de Tienda/ Dirección Social/RRHH deberá mantener al corriente del incidente al Departamento jurídico.

También aporta en ANEXO 5 documentos que comprenden:

- "*nota informativa videovigilancia (v.v.) CCTV de 2009"*, y 2010.

- "*nota informativa ejercicio de derechos y v.v. CCTV de 2013".*

Ambas son especies de guías internas informativas sobre videovigilancia en sedes, plataformas y puntos de ventas, o una nota informativa sobre la Ley Ómnibus

Como ANEXO 6 aporta un "*Manual de buen uso de los sistemas de información*" que es una especie de guía interna del grupo y un ANEXO que no tiene número pero que con el título "*Departamento de seguridad: Medios humanos"* indica:

4. Departamento de Seguridad: Medios Humanos
"*En Puestos Básicos*"
4.1. 2 *Operador Centro de Control*

Este puesto será considerado básico en aquellos Hipermercados en los que cuenten con CCTV. Su finalidad principal será la atención de alarmas y la de detección y prevención en todos los espacios del Hipermercado de actuaciones anómalas por parte de las personas que se encuentre en el Hipermercado.

En este puesto podrán estar ubicados además del CCTV, la Central de Alarmas Anti-Intrusión, la Central de Alarmas Contra Incendios, la Central de Alarmas Técnicas.

Las principales labores para llevar a cabo en este puesto serán las siguientes:

1. Comunicación al resto del Equipo de Seguridad y Servicios Auxiliares de los saltos de alarmas de intrusión y contra incendios que se produzcan para su comprobación. Se intentará, si ello fuese posible utilizando el sistema de CCTV, la valoración inmediata del citado salto, aportando la información necesaria al resto del equipo. Una vez comprobadas las causas del salto de alarma, se procederá a su rearme.

2. Comunicación al Equipo de Mantenimiento de los saltos de alarmas técnicas y contra incendios.

3. Control a través del CCTV de todas las zonas del Hipermercado, extremando la atención sobre aquellas que estén más afectadas por los hurtos externos e internos y sobre aquellas en las que se detecte que aparece una mayor cantidad de etiquetas de seguridad arrancadas.

4. Seguimiento de personas sospechosas o reincidentes durante su estancia en la sala de ventas.

5. Enlace y coordinación a través de la emisora base o teléfonos inalámbricos y CTV, de los Equipos de Servicios Auxiliares (Seguridad, Mantenimiento, Limpieza...) así como en su caso atención telefónica general y gestión del equipo de megafonía. Esta función es especialmente relevante en situaciones de emergencia ya que en este tipo de situaciones el Centro de Control debe convertirse en Centro de Coordinación de Emergencias. El plan de actuación en caso de emergencias debe ser conocido por todo el personal de seguridad y servicios auxiliares y participarán en los simulacros establecidos.

4030 puestos: Responsable de Seguridad

Será el encargado de garantizar el correcto funcionamiento de los puestos anteriormente citados. Es el interlocutor habitual ante la empresa de seguridad y las Fuerzas y Cuerpos de Seguridad del Estado. Apoyará en las intervenciones, aporta al Gerente aquellas ideas que puedan mejorar la seguridad del Hipermercado y presenta mensualmente sus propuestas de mejora al Equipo de Dirección. Trimestralmente presenta además un informe a dicho equipo con las incidencias producidas en dicho período.

Labores específicas para realizar serán las siguientes:

1. Coordinar y formar al equipo de seguridad, manteniendo una formación continua en todas las materias relacionadas por seguridad.

2. Controlar que cada uno de los miembros del equipo de seguridad está perfectamente enterado de las funciones de su puesto.

3. Realizar cuantas pruebas fueran necesarias para calibrar el grado de eficacia tanto del equipo de seguridad como de los medios técnicos con los que cuenta el hipermercado.

4. Mantener reuniones diarias con el Gerente, a quien informará de las incidencias del día anterior. Ante una incidencia grave, informará urgentemente al Gerente.

5. Apoyar al equipo de seguridad en las necesidades que se produzcan.

6. Controlar las cesiones internas…

10. Coordinar y asignar a los diferentes puestos las nuevas misiones (temporales o indefinidas) que se vayan elaborando para el equipo de seguridad.

11. Informar de las incidencias detectadas en los medios técnicos para su reparación, manteniendo un seguimiento de estas incidencias hasta su total resolución.

12. Encargar los pedidos de etiquetas de seguridad y gestionar los mismos.

13. Controlar que se cumplen los procedimientos de alarmado de los productos, tanto en la cantidad de artículos a alarmar como en el buen alarmado, coordinando con los Jefes de Área las modalidades y necesidades de alarmado…

16. Mantener reuniones periódicas con el Equipo de Dirección para la creación, seguimiento y evaluación de nuevos procedimientos de alarmado y de vigilancia, así como para su intervención en todos aquellos procesos de cambio dentro del Hipermercado que puedan afectar a los procedimientos de seguridad.

17. Mantener los contactos necesarios con los Cuerpos y Fuerzas de Seguridad del Estado, con las Policías Autonómicas (en su caso), con las Policías Locales, con Bomberos y Protección Civil…

20. Elaborar, sobre la base de las indicaciones del Gerente, los presupuestos del Departamento de Seguridad y gestionar los mismos.

Las ausencias del Responsable de Seguridad serán cubiertas por la persona que designe por escrito el Gerente del Hipermercado.

La necesidad de minimizar los costes operativos puede provocar la eliminación del puesto de Responsable de Seguridad, siendo el mismo asumido por el Gerente del Centro quien podrá delegar parte de las funciones propias del Responsable de Seguridad en alguno de

los miembros del Servicio de Seguridad, o en otro miembro del equipo directivo del Hipermercado.

Evidentemente aquellos Hipermercados en los que desaparezca la figura del Responsable de Seguridad se deberán modificar los procedimientos en los que éste intervenía físicamente.

Algunos de ellos se reseñan a continuación, debiendo el Gerente adaptar en su caso aquellos otros en los que estuviese implicado el Responsable de Seguridad:

g) Documentación de las funciones y obligaciones del personal con acceso a las grabaciones del sistema de videovigilancia. Relación nominativa y detallada de dicho personal junto con los documentos firmados de aceptación de las mencionadas funciones y responsabilidades. Si el acceso estaba permitido a terceros, indicar la finalidad de dicho acceso y las funciones que tuvieran encomendadas, adjuntando copia del contrato correspondiente.

Manifiestan que dicha información deberá ser proporcionada en su caso por CECOSA. "*En todo caso, se aporta como documental complementario, copia de la política de buen uso de los sistemas de información que aplicaba en 2011, como ANEXO 6".*

h) Aclaración de si el acceso al sistema se producía bajo una clave genérica o mediante accesos personalizados para cada individuo autorizado.

Responden que "*Entendemos que no, y ello pues en 2011, el acceso no estaba volcado en un sistema informático, en aquella época los sistemas eran videograbadores que no soportaban control de acceso lógico. En esta línea, recordamos que los supermercados no eran sujetos obligados a adoptar medidas de seguridad especificas en este campo. En suma, el modelo no permitía el acceso con clave*"

i) Información respecto a si se registraban los accesos a las imágenes del sistema de videovigilancia y si se realizaban auditorías sobre dicho registro al efecto de comprobar si se producían accesos no autorizados.

Responden que "*como se correspondían con datos de nivel básico, tampoco se registraban los accesos a las grabaciones, no se realizaban auditorías*

j) Política de gestión de soportes. Persona encargada de autorizar la salida de estos, en particular, en el caso de las grabaciones del sistema de videovigilancia.

Responde que, al ser datos básicos, "*conforme al reglamento de 2007, no mediaba registro de entrada y salidas como tal*."

k) Plazo definido de conservación de las imágenes registradas por las cámaras y mecanismos de borrado de las grabaciones obsoletas.

Indica que conforme se recoge en el ANEXO 4, no superando 30 días.

l) Posibles criterios definidos para la conservación de las imágenes más allá del plazo que establece la Instrucción 1/2006, de 8/11, 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. Describir el mecanismo de conservación seguido y el sistema donde se almacenan las grabaciones sujetas a estos criterios.

Indica que, si existía un motivo que justificara esa conservación más allá del plazo, se llevaba a cabo y siempre conforme al protocolo de tratamiento de la imagen de videovigilancia.

m) Descripción de la cadena de custodia seguida por el responsable del sistema de videovigilancia y el servicio de seguridad que estaba contratado en el caso de producirse la extracción de grabaciones.

Indica que era la empresa responsable del servicio de seguridad la encargada de sacar las mencionadas grabaciones y quien tenía, mantenía y detentaba el poder de disposición.

n) Detalle del Centro de Control donde se realizaba la monitorización y la grabación de las imágenes, especificando las medidas de control de acceso al mismo.

Indica que este centro fue vendido en 2011 y todo este tipo de información se entregó al comprador. Estos elementos de seguridad se entregaron al comprador y el vendedor no se queda con copia-por seguridad- "*En consecuencia se entregaron las instalaciones con los elementos ad hoc*"

o) Para todos los puntos anteriores recogidos en este apartado, deberá describir en detalle cuál es la política seguida en la actualidad en los centros comerciales EROSKI que permanecen operativos, así como descripción completa de la arquitectura de los sistemas de videovigilancia actualmente implantada (sistemas de monitorización y grabación, modo de operación, acceso local o remoto, …)

Responde que adjunta ANEXO 7 que contiene el protocolo de videovigilancia año 2012 que establece como se actúa hoy y que extiende su ámbito de aplicación a todos los puntos de venta y no solo a los centros comerciales.

p) Información respecto a las posibles cesiones realizadas de las grabaciones objeto de investigación a terceras partes (Fuerzas y Cuerpos de Seguridad del Estado, Órganos Judiciales, Organismos Públicos…) indicando el mecanismo seguido para documentar quién autorizó la cesión y las condiciones en que esta se produjo. Aclarar cuál es la política seguida en la actualidad en los centros comerciales de la sociedad que permanecen operativos en relación con este respecto.

Responde que no le consta que se produjese extracción alguna de las grabaciones ni comunicación a terceras partes. Precisa que en la actualidad y siempre se ha esperado al requerimiento oficial y solo entonces se extrae. Aporta *VHP seg extracto*, en ANEXO 8 puntos 4.1.2 y 4.3 "*en el que describimos la operativa del centro de control y del responsable de seguridad en nuestro caso externo*".

Apunta a la empresa responsable del servicio de seguridad como la encargada de extraer las grabaciones aunque, en el protocolo de tratamiento de la imagen, esta no figura entre la relación tasada de usuarios con acceso a los datos y el propio contrato, en la estipulación *DECIMOQUINTA* relativa a la confidencialidad recoge que *"Exclusivamente la Propiedad, en coordinación con el Contratista, o viceversa, podrá conceder, alterar o anular el acceso autorizado sobre los Sistemas de Videovigilancia"* y que *"Si en algún momento, los soportes mencionados en el apartado anterior (grabaciones en disco o cinta) salieran fuera de los locales donde se lleva a cabo la prestación del servicio, esto requerirá autorización por parte de la Propiedad"*, no habiéndose aportado ningún documento que acredite esa delegación de funciones en un tercero o que dicho acceso fuera expresamente autorizado por CECOSA como responsable del sistema. Aclara que la forma de proceder, tanto en 2011 como en la actualidad, en el caso de que sean solicitadas imágenes, es esperar al requerimiento oficial y sólo en ese momento se produce la extracción.

q) Si el sistema de videovigilancia estaba conectado a una Central Receptora de Alarmas (CRA) con una serie de cuestiones relacionadas como por ejemplo la identificación de la empresa de seguridad que realizó la instalación de las videocámaras y copia del contrato de prestación de servicios firmado, manifestando que como el centro no es de su propiedad ni la empresa proveedora de la instalación existe, no pueden contestar la cuestión

SÈPTIMO: Con fecha 23/05/2018, al objeto de comprobar cómo se realiza en la práctica la gestión de los sistemas de videovigilancia, se efectúa una visita de inspección en un hipermercado de EROSKI gestionado por CECOSA situado dentro del "*Centro Comercial Luz del Tajo*", en el término municipal de Toledo.

Durante la inspección, el Gerente del establecimiento pone de manifiesto que el sistema de videovigilancia empezó a funcionar en el año 2004, cuando se abrió. Manifiesta que la instalación y el mantenimiento lo realizó una empresa llamada INGECOM, siendo la finalidad del sistema la seguridad y evitar hurtos.

Queda emplazado el Gerente, al no tener en las oficinas copia de la documentación, a remitir a esta Agencia copia de dicho contrato.

Con fecha 29/05/2018 tiene entrada escrito de CECOSA aportando la copia de contrato suscrito con la sociedad INGECOM SISTEMAS, S.L. cuyo objeto es el mantenimiento de los sistemas de CCTV y anti-intrusión instalados en una relación de centros del GRUPO EROSKI que se listan en un anexo al contrato que no se acompaña. Se aprecia que dicho contrato se circunscribe a tareas de mantenimiento preventivo, correctivo y suministro de nuevos equipos en sustitución de otros ya existentes, pero no se hace ninguna referencia a las tareas de instalación original del sistema de videovigilancia, no pudiendo confirmar que INGECOM se haya encargado de dicho cometido.

Sí se aprecia en el contrato, de acuerdo con el apartado 4. PROCEDIMIENTO DE TRABAJO, que en los trabajos realizados por el servicio de asistencia técnica de INGECOM a raíz de las incidencias surgidas en los equipos e instalaciones objeto del contrato y comunicadas por escrito por el GRUPO EROSKI, la empresa de mantenimiento debe rellenar un parte de trabajo con la descripción detallada de la actuación realizada que deberá ser firmado por el responsable del Centro en el que se realice la actuación o por personal de este en el que se delegue. Incorpora también, en la estipulación décima relativa a la *CONFIDENCIALIDAD*, un compromiso de protección de datos personales en el que ambas partes acuerdan que, *"toda información relativa a datos de carácter personal de la propiedad, a la que la empresa tenga posibilidad de acceso, con ocasión de la prestación del servicio objeto de este contrato, es de carácter confidencial a todos los efectos y sujeta, en consecuencia, al más estricto secreto profesional"*, sometiéndose ambas partes expresamente, en lo que a legislación aplicable se refiere, *"a lo establecido en la LOPD y demás disposiciones en materia de protección de datos existentes."*.

-Tienen contratado servicios de seguridad y vigilancia con la empresa OMBUDS. El servicio se realiza por un jefe de equipo y un vigilante de seguridad, encargados de cubrir los turnos de mañana y tarde, más personal auxiliar que realiza otras tareas como el *alarmado* de productos. Indica que dicho personal de seguridad está presente durante el día pero que una vez cierra el establecimiento comercial se procede al alarmado del sistema de seguridad y el servicio de vigilancia en horario nocturno es cubierto de forma remota por la empresa SABICO que realiza las funciones de CRA (Central Receptora de Alarmas) y que se conecta de forma remota para verificar, a través de las cámaras y las grabaciones registradas por estas, los saltos de alarma producidos en las instalaciones.

Se aporta, el 29/05/2018, copia del contrato de fecha 4/05/2009 suscrito entre la sociedad investigada y la empresa de seguridad que ya obraba en poder de esta Agencia y

donde se confirma que también da cobertura, dentro del listado de centros que figuran en el anexo, al establecimiento EROSKI LUZ DEL TAJO (TOLEDO).

-La instalación de videovigilancia está señalizada mediante carteles informativos que responden al modelo de cartel al que hace referencia la Instrucción 1/2006 de esta Agencia, encontrándose tres de ellos a la entrada del hipermercado, otro en el interior del mismo en la zona de perfumería, otro en la caja central y zona de atención al cliente, uno más en la tienda de óptica anexa al hipermercado y el último, en el cuarto de intervención, en el que además existe una cámara, y que es donde se acompaña a las personas sospechosas de cometer hurto de algún producto dentro del establecimiento con el ánimo de resolver el incidente.

-El sistema de videovigilancia, se compone de un total de 58 cámaras ninguna de las cuales realiza grabación de sonido, de las cuales 10 son de tipo domo con zoom y capacidad de movimiento y el resto fijas, y repartidas por toda la superficie del hipermercado sin que existan cámaras en el exterior.

-Según manifiestan los representantes de CECOSA, el Gerente y el jefe de equipo de seguridad y se comprueba posteriormente, las imágenes registradas por las cámaras se visualizan desde un monitor ubicado:

. en el despacho del Gerente,

. en el puesto de control o pódium situado a la entrada del hipermercado y

. desde el centro de control que es donde además se localiza el sistema de grabación compuesto por tres grabadores de 16 canales cada uno de ellos, capaces de almacenar las grabaciones de un total de 48 cámaras, de modo que las imágenes captadas por las 10 cámaras restantes sólo pueden visualizarse en tiempo real.

Indican que a la visualización de las imágenes tienen acceso el Gerente y el personal de seguridad.

Según refieren, el sistema funciona en modo de grabación continua, conservándose las imágenes por un período aproximado de 10 o 15 días sobrescribiéndose en disco las imágenes más antiguas con otras nuevas una vez superado el plazo de conservación. Para

conectarse al sistema de grabación es preciso introducir un usuario y una contraseña, estando definidos varios perfiles, entre ellos:

. dos perfiles administradores,

. un perfil gerente,

-un usuario Eroski, y

. un perfil seguridad.

Manifiesta CECOSA que *"El jefe de equipo de la empresa de seguridad accede al sistema utilizando tanto el usuario seguridad como el usuario gerente y cuando el Gerente necesita acceso a las imágenes grabadas se le requiere al personal de la empresa de seguridad que es el que realiza el acceso o en su caso la extracción".*

-Si se produce algún incidente de seguridad, el personal de la empresa de seguridad realiza el seguimiento del sospechoso esperando a la persona en línea de caja para invitarle a que abone los productos sustraídos. Si no accede al pago de estos se le acompaña al cuarto de intervención, que está situado detrás de la zona de caja central y atención al cliente, solicitándole de nuevo que abone los productos. Sólo si rehúsa el pago se requiere la intervención de la Policía y es el Gerente el que interpone la correspondiente denuncia, lo que coincide con lo reflejado en el procedimiento operativo ante robo, hurto o roturas del *"Manual Operativo del Servicio de Seguridad"* facilitado por OMBUDS. Por su parte, el servicio de seguridad, tal y como recoge el manual operativo, tiene la obligación de cumplimentar diariamente un parte o informe donde deja constancia de todos los incidentes ocurridos conservando de forma indefinida, según manifiestan, dichos partes en el centro de control y entregando una copia de este al Gerente que, una vez revisado, procede a su destrucción. Durante las comprobaciones efectuadas se constata que en una de las estanterías del centro de control se conservan apilados un importante volumen de partes diarios. Se selecciona por muestreo el último de la pila y se solicita su exhibición, comprobando que se corresponde con un parte de fecha 2/01/2009 que en las anotaciones no hay consignados datos de carácter personal.

-Solicitado que se aporten procedimientos documentados en el marco de las tareas de videovigilancia, el Gerente y el Jefe de equipo de seguridad refieren que "*no existe ningún protocolo documentado, ni de los usuarios y perfiles de acceso así como ningún documento firmado en el que se recojan las responsabilidades y aceptación de funciones del personal*", aportando como única información escrita y documentada un manual de EROSKI denominado *"Manual de Orientación Profesional para Vigilantes de Seguridad"* que regula los procedimientos de actuación de los vigilantes de seguridad ante situaciones conflictivas con clientes y empleados pero en el que no se hace ninguna referencia a los procedimientos operativos, las funciones, cometidos y responsabilidades del personal de la empresa de seguridad en materia de videovigilancia. Sin embargo, entre la información facilitada por OMBUDS en respuesta al requerimiento del 30/05/2018 al solicitar documentación que acredite que los vigilantes de seguridad conocen los procedimientos a seguir y han aceptado sus funciones y responsabilidades en materia de videovigilancia, se facilita una muestra de treinta documentos firmados de información y aceptación de funciones por parte del personal de seguridad, todos ellos de idéntico contenido y entre los que no es posible confirmar que se encuentren los correspondientes al personal de seguridad que presta servicios en el establecimiento EROSKI inspeccionado al desconocer los datos

identificativos del Jefe de equipo y el vigilante de seguridad, en los que se recogen las obligaciones a seguir derivadas del acceso a los datos de carácter personal durante el desarrollo de sus funciones junto con una referencia a las medidas de seguridad que deben conocer y cumplir y entre las que se indica textualmente *"Hacer uso de los mecanismos facilitados por el encargado para identificar y autenticar de forma inequívoca y personalizada a los usuarios del sistema. Cada Vigilante debe poseer una clave de acceso única y personal que debe custodiar oportunamente".*

-Durante la inspección a las instalaciones se verifica:

-Hay una zona de oficinas en la que está ubicada el despacho del Gerente, y en el mismo existe un monitor desde el que es posible la visualización de las imágenes.

-Existe una zona de acceso restringido solo al personal en la que se sitúa el centro de control de seguridad, el cuarto de intervención, el acceso a la zona de caja central y mostrador de atención al cliente. El acceso a dicha zona se realiza a través de una puerta, permanentemente cerrada, de la que sólo tiene llave, según manifiestan, el jefe de equipo de la empresa que presta servicios de seguridad pero la cual también es posible abrir mediante un pulsador situado en la caja central y que es accionado por el personal que se encuentra en esa zona cuando alguien del establecimiento necesita acceder. Una vez sobrepasada dicha puerta y ya dentro de la zona de acceso restringido, todos los cuartos, incluido el centro de control donde se ubican los monitores y los sistemas de grabación, se encuentran con las puertas abiertas, sin ninguna medida de control de acceso físico, siendo posible acceder a dicha estancia y a los sistemas de monitorización (5 monitores) y grabación (3 grabadores) en ella ubicados. Dicha forma de proceder es contraria a lo descrito en las *Notas Informativas relativas a la gestión de la seguridad en materia de protección de datos de carácter personal en videovigilancia y CCTV en Sedes, Plataformas y Puntos de Venta* facilitadas tanto por CECOSA como por EROSKI SC en sus respuestas a los requerimientos de información realizados por esta Agencia y donde, en el apartado relativo a los requisitos para la instalación y uso de un CCTV, se indica que *"El visionado de las imágenes debe hacerse en un área de acceso restringido y sólo estará habilitado para ello el personal autorizado de tienda, sede o plataforma y/o a personal de la empresa de seguridad"* así como que *"La emisión en tiempo real de las imágenes no puede reproducirse en pantallas visibles por cualquier cliente o personas no autorizadas".*

- Se verifica que el acceso a las imágenes grabadas se realiza a través del software del grabador, siendo necesaria la identificación y autenticación mediante la introducción de un código de usuario y una contraseña. Se comprueba la existencia de cuatro perfiles siendo dos de ellos administrador. Se accede al software de gestión con el perfil de gerente y se comprueba que en los tres grabadores las imágenes más antiguas conservadas corresponden al día 17/05/2018. Se comprueba que seleccionando una cámara y un

intervalo de fechas, el software de gestión del grabador permite la extracción de las imágenes seleccionadas a un soporte externo.

-Los Inspectores comprueban que sobre uno de los monitores hay pegado un pos-it que contiene el código de usuario administrador y la contraseña. Se solicita el acceso con dichos códigos comprobando que permiten el acceso al software de gestión de grabaciones. En presencia de los inspectores actuantes, dicho papel es destruido por el jefe de equipo de seguridad. En doc. 2 figura la fotografía de dicho post it que posibilita el acceso al sistema.

-Una vez dentro del cuarto destinado a centro de control se aprecia que en una de sus paredes se exhiben, en modo mosaico, numerosas fotografías de personas sospechosas de cometer ilícitos, algunas de las cuales datan del año 2005, según muestra incorporada como prueba al expediente de referencia y que de acuerdo a las aclaraciones facilitadas por el Gerente del establecimiento en conversación telefónica posterior e incorporada mediante diligencia a las actuaciones de inspección de referencia así como de las anotaciones y datos que figuran en las fotografías incorporadas tomadas durante las inspección, proceden de la Policía, de otros centros comerciales e incluso de otros operadores y llegan normalmente por email. Si son del sistema de grabación del propio establecimiento, dado que en el centro de control no hay ordenador ni impresora, son extraídas a un dispositivo externo tipo USB y se imprimen en alguno de los equipos utilizados por el personal de EROSKI. Se recogen fotografías de la mencionada pared en la que figuran unas 15 más o menos, observándose que en una de ellas aparece un individuo con su huella dactilar, los individuos aparecen en el interior de hipermercados o del centro comercial, algunas con anotaciones manuales, otras parecen extraídas de sistemas de videovigilancia.

- Manifiestan que, cuando el Gerente necesita acceder a las imágenes de alguna de las grabaciones del sistema, se lo requiere al personal de la empresa de seguridad que es el que realiza el acceso y, en su caso, la extracción de las imágenes, a través del puerto USB con el que cuentan los grabadores, a un soporte externo, seleccionando para ello, según demostración realizada por el Jefe de equipo de seguridad, la cámara que registró las imágenes solicitadas y el intervalo de fechas requerido.

El Servicio de Inspección solicita que aporten:

- copia de contrato suscrito con INGECOM de instalación y mantenimiento del sistema de videovigilancia.

-copia de contrato de prestación de servicios con SABICO en los servicios de televigilancia.

OCTAVO: Con fecha 24/05/2018 y al objeto de obtener datos de carácter técnico en relación con la instalación del sistema de videovigilancia del establecimiento comercial EROSKI situado en el Centro Comercial Luz del Tajo inspeccionado, se solicita información a INGECOM SISTEMAS, S.L, a la que CECOSA identificó como empresa instaladora y que mantiene dicho sistema, teniendo entrada en esta Agencia, escritos de 4 y 18/06/2018 respectivamente, en los que aporta idéntica copia del contrato a la ya facilitada por CECOSA y en el que aclara, en relación a si tienen acceso a las grabaciones, que tiene acceso, sólo previo requerimiento del departamento de seguridad de su cliente que, en algunas

ocasiones y previa orden de trabajo de las que se aporta ejemplos, ha solicitado la retirada "*in situ*" de un clip de imagen, prestando en ese caso el servicio de extracción técnica y entregando a la persona designada por su cliente un soporte externo con las imágenes obtenidas del grabador, pero sin que INGECOM retenga copia de las mismas. Indican que es posible la configuración del grabador de forma remota y que el mantenimiento de los sistemas de seguridad, incluidos los grabadores, exige un acceso bidireccional que es realizado por la empresa SABICO que gestiona la central receptora de alarmas.

Aportan datos técnicos con relación a la instalación y entre los que se incluyen las marcas y modelos de las cámaras y los grabadores. De estos aclaran que funcionan en modo de grabación continua con sobreescritura, siendo necesario para acceder disponer de un usuario y una contraseña.

Identifican los perfiles configurados para acceder a los sistemas de grabación comprobando que todos ellos están habilitados para realizar el visionado directo de las cámaras, así como la reproducción de las imágenes previamente registradas, con la salvedad del perfil administrador que adicionalmente permite la configuración de los sistemas y que es utilizado por INGECOM como empresa de mantenimiento. Aclaran que el acceso a los grabadores, además de localmente a través de los monitores directamente conectados, se puede realizar desde la red local de EROSKI, identificando en la planimetría aportada en el despacho del Gerente, un monitor y un pc con una consola de control que, según manifestaciones del técnico de INGECOM incorporadas mediante diligencia a las actuaciones de inspección de referencia, permitiría conectarse en remoto a los grabadores, desplazarse por las grabaciones registradas e incluso extraer imágenes, además a través de una Red Privada Virtual (VPN) que, en esas mismas aclaraciones, permite el acceso desde el exterior a la red de EROSKI si se cuenta con el software de conexión y se dispone de usuario y contraseña.

NOVENO: Con fecha 5/06/2018 se registra entrada de escrito en respuesta a la petición de información de esta AEPD, de 22/05/2018, por parte de SABICO, empresa inscrita en el Registro de Empresas de Seguridad de la Dirección General de la Policía, identificada como la encargada de prestar el servicio de control de alarmas nocturno y video verificación en el hipermercado de la marca comercial EROSKI situado en el Centro Comercial Madrid Sur, EROSKI VALLECAS, en el que se solicitaba:

1. Copia del contrato de prestación de servicios suscrito entre SABICO y la sociedad titular del establecimiento comercial, indicando si la instalación de las cámaras de videovigilancia la realizó SABICO o, por el contrario, otra empresa de seguridad, identificando en dicho caso a la empresa responsable de la instalación. Aportar copia de la documentación que permita comprobar que SABICO notificó las características de la instalación de videovigilancia a la autoridad competente en materia de seguridad privada.

SABICO facilita copia de un contrato de arrendamiento de servicios de seguridad de fecha 4/05/2009, de carácter anual renovable, suscrito con CECOSA cuyo alcance consiste

en el establecimiento de una conexión a la central receptora de alarmas que gestiona SABICO para una relación de centros de la marca comercial EROSKI que figuran en un anexo del contrato. Analizado el contrato, y pese a que en el documento "*Tratamiento de la Imagen"* facilitado tanto por EROSKI SC como por CECOSA refiere que hay empresas que, por los servicios que prestan, acceden a las imágenes del sistema de videovigilancia motivo por el cual *"se convertirá en encargada del tratamiento según la LOPD y así deberá constar en el contrato que será obligado suscribir con el proveedor",* en el contrato suscrito con **SABICO** no se consigna ninguna de las condiciones que el artículo 12 de la Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal establece para regular las condiciones de servicio en el acceso a datos por cuenta de terceros.

2. Indicar si SABICO tenía acceso a las grabaciones del sistema de videovigilancia del establecimiento comercial, describiendo con detalle las características de la solución tecnológica utilizada (grabación continua, programada o activada por eventos, ubicación física del sistema de grabación, modo de almacenamiento de las grabaciones realizadas y plazo de conservación de las mismas, acceso local o remoto a las imágenes, sistema de control de acceso de los usuarios autorizados, mecanismo de borrado de las grabaciones obsoletas,…) y las condiciones o criterios bajo los que se producía dicho acceso. Deberá además facilitar información sobre si:

- la conexión y el acceso a las grabaciones se producía bajo una clave genérica o mediante accesos personalizados para cada empleado de SABICO encargado de prestar el servicio de seguridad.

- se registraban los accesos realizados a las imágenes grabadas por el sistema de videovigilancia

- se realizaban auditorías sobre dicho registro al efecto de comprobar si se producían accesos no autorizados, identificando a la persona encargada de realizar dichas comprobaciones.

Según refiere SABICO, el sistema estuvo conectado hasta el 19/09/2011, y consistía en un panel de intrusión y un sistema CCTV instalado por la empresa EKINTZA y al que SABICO accedía de forma remota, mediante login y contraseña, utilizando una aplicación específica configurada por CECOSA y sin realizar ningún tipo de almacenamiento de las imágenes registradas por el sistema.

Matizan que el acceso a las grabaciones por parte de SABICO se circunscribía exclusivamente a la verificación de los saltos de alarma producidos en las instalaciones de CECOSA**.** en el horario en el que el local comercial tenía cerrado el acceso al público y los empleados habían abandonado el establecimiento; acceso realizado siempre, según manifiestan, conforme a las buenas prácticas establecidas en el sector sobre el funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, aunque como se ha indicado, el contrato aportado no incorpora ninguna cláusula que regule la

prestación de servicios ni establezca condiciones desde el punto de vista del acceso a datos de carácter personal.

Indican que también era posible acceder al sistema bajo demanda y requerimiento del responsable de CECOSA, para proporcionar aquellas grabaciones de los saltos de alarma del sistema con mayor duración de la obtenida en la señal asociada a las alarmas, aunque aclaran no tener constancia de haber sido requeridos para extraer imágenes bajo esta última modalidad. Refieren que SABICO no accedió a las grabaciones del sistema publicadas en los medios de comunicación por lo que en ningún momento pudo facilitar copia de estas a terceros.

DÉCIMO: Con fecha 30/05/2018 y habida cuenta de que, tal y como se incorpora mediante diligencia a las actuaciones de inspección de referencia, aun tratándose de personas jurídicas diferentes ha habido una relación entre la sociedad *EKINTZA* encargada de realizar la instalación del sistema de videovigilancia en el establecimiento comercial *EROSKI* donde tuvieron lugar los hechos publicados en los medios de comunicación, y la empresa INGECOM, encargada de la instalación de videovigilancia en el establecimiento comercial *EROSKI* inspeccionado el 23/05/2018, se solicita a esta última sociedad que facilite toda la información relativa a las características técnicas de la instalación que aún puedan obrar en su poder, teniendo entrada en esta Agencia, escritos con fecha 7 y 13/06/2018, de INGECOM en el que facilita la identificación de una persona, socio de EKINTZA e ingeniero de dicha mercantil quién, según se refiere, ha manifestado su plena disponibilidad para aclarar toda la información técnica que corresponda, aportando junto a dicho escrito la planimetría del sistema CCTV y de los elementos de seguridad del establecimiento comercial EROSKI VALLECAS situado en el Centro Comercial Madrid Sur así como una breve descripción técnica de su funcionamiento.

En los planos se observa que, la matriz de conexión de las cámaras y los sistemas videograbadores estaban situados en planta baja, en un espacio situado dentro de la zona de caja central, y donde no se marca la existencia de ningún monitor. En entreplanta, en la zona de oficinas, se situaban dos cuartos que se correspondían con la recepción y un cuarto no identificado, donde existían hasta seis monitores de visualización del sistema y las consolas de control que permitían el seguimiento de personas por el establecimiento haciendo uso de las diferentes cámaras dispuestas por toda la superficie comercial. En un tercer cuarto, ubicado en entreplanta y que se identifica como el despacho del Gerente del establecimiento, se sitúa un ordenador con un software instalado que permitía, al igual que desde el frontal de los grabadores, la navegación por las grabaciones registradas por el sistema de videovigilancia en busca de eventos concretos.

DECIMO-PRIMERO: Con fecha 13/06/2018, tal y como se incorpora mediante diligencia a las actuaciones de inspección de referencia, se mantiene una conversación telefónica con el representante de INGECOM con el objetivo de obtener una aclaración, por parte del que era ingeniero de EKINTZA del informe técnico remitido, aprovechando el representante a manifestar verbalmente su ofrecimiento de comparecer voluntariamente junto con el ingeniero en la sede de esta Agencia para ampliar la información facilitada por escrito y dar respuesta a todas las cuestiones que se planteen.

El 25/06/2018, se mantiene una reunión con ambos en la sede de la AEPD, incorporando al expediente copia del acta voluntaria de comparecencia. Durante la reunión, el ingeniero confirma que la ya extinta sociedad EKINTZA**.** se encargó de la instalación y mantenimiento del sistema de videovigilancia del establecimiento comercial EROSKI Vallecas situado en el Centro Comercial Madrid Sur hasta que en 2012 quebró dicha sociedad. Aporta copia impresa de la información ya remitida en la respuesta del

requerimiento de 30/05 y donde se sitúan los distintos elementos del sistema de videovigilancia, manifestando que, en la sala de seguridad donde se ubicaban los sistemas grabadores, aunque no aparecen identificados monitores, debían de existir. Indica que el acceso a los sistemas de grabación y la extracción de las imágenes se producía tanto de forma local como de forma remota por parte de EROSKI, bien desde el PC ubicado en el despacho del Gerente como a través de una VPN desde la Central de EROSKI en Elorrio. También se producían accesos en remoto tanto por la empresa encargada de realizar la gestión de las alarmas a fin de verificar lo ocurrido si se producía un salto de alarma como por parte de la propia EKINTZA que realizaba el mantenimiento de los sistemas. En ese caso, el acceso siempre se producía bajo órdenes de servicio para verificar el correcto funcionamiento de los dispositivos o realizar una extracción de imágenes como soporte técnico al cliente si así lo solicitaba.

Manifiesta que, habida cuenta del estado de la tecnología, aunque existían distintos perfiles de usuario para realizar los accesos, no quedaba registro de estos y que la conservación de las imágenes, contando que se trataba de una instalación del año 2011 y de tecnología analógica, estaría en torno a los 15 o 20 días en el caso de las grabaciones generales. En el caso de que se produjese un robo, hurto o cualquier otro delito del que fuera preciso aportar pruebas, las imágenes extraídas y su conservación eran gestionadas por el propio cliente.

DECIMO-SEGUNDO: Con fecha 13/06/2018 tiene entrada un escrito de la DIRECCIÓN GENERAL DE LA POLICÍA, de respuesta a una petición de información de 15/05/2018, en la que se remitía una reseña de una noticia del diario digital EL MUNDO de 26/04/2018, para que informara sobre:

1) Descripción completa del procedimiento general seguido por el Cuerpo Nacional de Policía cuando, a raíz de un incidente, particulares o empresas realizan una llamada al servicio de emergencias denunciando un posible delito y requiriendo la presencia policial. Deberán indicarse, ordenadas temporalmente, la relación completa de actuaciones realizadas por todas las partes intervinientes en el procedimiento de atención de un incidente, detallando, entre otros aspectos:

-Modo en que se registran y almacenan las comunicaciones realizadas entre la persona, física o jurídica, que denuncia el incidente y el centro de coordinación que atiende la llamada de emergencia.

-Modo en que se registran y almacenan las comunicaciones entre el centro de coordinación que atiende la llamada de emergencia y los agentes del coche patrulla que se desplaza al lugar del posible incidente.

-Descripción completa y detallada de toda la documentación generada por los Agentes de Policía desplazados, tanto en el lugar de los hechos como de vuelta a las dependencias policiales una vez atendida la situación que ha requerido su presencia.

-Detalle y características del sistema de registro documental y de archivo físico utilizado para guardar copia completa de la documentación generada y de las evidencias o pruebas obtenidas relacionadas con el incidente atendido, especificando:

-Carácter local (por Comisaría) o centralizado (Dirección General de la Policía u otro órgano en la estructura del Ministerio del Interior) del sistema de registro documental y archivo utilizado.

-Plazo de conservación definido para las entradas creadas cuando se registra un incidente.

-Identificación de los posibles tipos de acceso al sistema y de los perfiles asociados.

-Descripción de las medidas de seguridad establecidas para controlar los accesos al sistema de registro y archivo, así como del procedimiento de cadena de custodia definido para garantizar que no se producen accesos ni salidas de información, evidencias y pruebas no autorizadas.

Manifiestan que, bien se reciba la llamada en la Sala 091, bien directamente en la Comisaría de Distrito, esta queda registrada en las aplicaciones informáticas o en el libro de telefonemas, respectivamente, según el medio por el que se notifique el aviso. Aclaran que el indicativo policial comisionado para comprobar la veracidad de los hechos e identificar a la persona retenida por los vigilantes de seguridad sólo procedería a su detención en caso de que el hecho revistiese carácter de delito, procediendo al traslado de la persona a las dependencias policiales para la realización de las oportunas diligencias que quedan registradas. En todo caso, los agentes actuantes, al final de la jornada laboral, recogen los hechos en un "*parte de servicio*" que se conserva durante un período de cinco años procediéndose a su destrucción trascurrido ese tiempo.

2) Descripción completa del procedimiento seguido en el caso concreto del incidente ocurrido en el establecimiento EROSKI VALLECAS con fecha 4/05/2011 al que se refieren las imágenes del Anexo 1 y atendido por Agentes de la Comisaría Puente de Vallecas, facilitando copia completa de las comunicaciones y la documentación generada a raíz de la intervención de los Agentes de Policía y aclarando si llegaron a intervenirse, en el momento de los hechos o posteriormente como parte de las pruebas del incidente acaecido en el establecimiento comercial, copia de las grabaciones registradas por las cámaras. En caso afirmativo, indicar quién tuvo acceso a las grabaciones una vez registradas y si se produjeron comunicaciones de estas a terceras partes, identificando, en ese caso, a los terceros que las solicitaran.

Indican que en relación a los hechos sobre los que se cuestiona, no consta ni en los registros de la Sala 091 ni en el libro oficial de telefonemas de la Comisaría de Distrito de Puente de Vallecas ningún asiento relativo a la recepción de una llamada realizada desde el establecimiento comercial en relación con el incidente, así como tampoco consta ningún parte de servicio sobre la intervención de ningún indicativo de dicha dependencia policial, matizando al respecto de la posibilidad de que los agentes policiales llegaran a intervenir copia de las grabaciones realizadas por el sistema de videovigilancia que sólo se tiene acceso a las mismas en el supuesto de que exista un ilícito penal y como consecuencia se proceda a la apertura de un atestado policial, en cuyo caso, se solicitaría al centro comercial implicado copia de las imágenes mediante oficio para su remisión a la Autoridad Judicial junto con el resto del atestado instruido al efecto.

DÉCIMO-TERCERO: Con fecha 14/06/2018 tiene entrada en esta Agencia escrito de respuesta de CECOSA HIPERMERCADOS, que coincide en gran parte con lo aportado por EROSKI SC, que se resume en:

-Sobre EROSKI VALLECAS, viene a dar idéntica contestación a las cuestiones planteadas y a aportar la misma información ya facilitada en el escrito de respuesta del requerimiento inicial remitido a la matriz de grupo, sin identificar a las personas que ostentaban los cargos de responsabilidad (Gerente/Jefe de tienda y Responsable de Seguridad) en el establecimiento comercial a fecha de 4/05/2011 ni a las que ostentaban la autoridad para autorizar y verificar los accesos a los espacios en los que se encontraban los sistemas de videovigilancia, alegando bien que no tienen acceso a esos datos al no formar parte de la plantilla, bien que el establecimiento fue vendido y toda la información se entregó al comprador, no conservando la entidad, por cuestiones de seguridad, ese tipo de información. Tampoco se facilita la relación nominativa del personal autorizado a acceder a las grabaciones del sistema de videovigilancia, ya fuera interno o externo a la sociedad, soporte documental de la posible delegación de funciones realizada por la sociedad responsable en entidades externas, ni los documentos firmados de aceptación de funciones y responsabilidades en lo que se refiere a dichos accesos, manifestando que, dado el tiempo transcurrido y que ese centro no les pertenece desde finales de 2011, no conservan documentación al respecto.

En este sentido y según la información facilitada por EROSKI SC y después confirmada y ampliada por CECOSA HIPERMERCADOS, S.L., se identifica a:

- una mercantil denominada *EKINTZA*, ya extinguida según consta en Boletín Oficial del Registro Mercantil de 17/06/2014 y que se incorpora mediante Diligencia a las actuaciones de inspección de referencia, como la empresa encargada de la instalación del sistema de videovigilancia, sin constar, según manifiestan, copia del contrato.

- una empresa denominada *SABICO* como encargada de la Central Receptora de Alarmas (CRA) y con capacidad de acceso remoto a las grabaciones del sistema y para la que, en el momento de dar respuesta a los requerimientos realizados por esta Agencia con fechas 26/04 y 22/05 tampoco aportan copia del contrato suscrito.

-Sobre el sistema implantado en CECOSA; Centro comercial Luz del Tajo, Toledo, manifiesta que en la actualidad y según la información facilitada, son cuatro las empresas que prestan servicios de seguridad a CECOSA HIPERMERCADOS, S.L., entre las que se identifica a la sociedad OMBUDS COMPAÑÍA DE SEGURIDAD, S.A.

Aporta copia de un contrato marco de 26/04/2014 de "*arrendamiento de servicios seguridad y vigilancia*" entre las distintas empresas del Grupo y OMBUDS, siendo un contrato marco de prestación de servicio que abarca a centros comerciales del grupo EROSKI entre los que se encuentra el mencionado. Además de dicho contrato, se menciona que también existe como regulatorio del servicio un pliego de condiciones técnicas, un ANEXO I con servicios a prestar por el contratista y unas normas generales.

Ni en el mencionado contrato marco ni en los pliegos de condiciones del servicio del grupo EROSKI de 11/02/2014 se especifica la prestación del servicio de acceso a imágenes del sistema de videovigilancia, formas de accesos, protocolos, órdenes y funciones del personal, tan solo hay referencias genéricas a la posibilidad de dichos accesos en el contrato marco. Ni siquiera en los servicios a prestar por OMBUDS figura como modalidad el citado sistema ni en concreto especificado para el centro comercial Luz del Tajo

Respecto a las características técnicas particulares de la solución implantada y las medidas de seguridad físicas y organizativas existentes, las sociedades requeridas no aportan información más allá de la copia de un documento identificado como *"Tratamiento de la Imagen"* y que asocian al protocolo de videovigilancia, en su versión vigente en el momento de los hechos así como la versión actual del mismo, junto con otros documentos,

de carácter interno, en materia de videovigilancia y que recogen la forma de proceder en la captación y tratamiento de las imágenes, el procedimiento a seguir si algún cliente solicita el ejercicio de sus derechos así como el protocolo de actuación con las Fuerzas y Cuerpos de Seguridad.

En dicho protocolo de tratamiento de la imagen, en la finalidad de seguridad privada, identifica la relación tasada y limitada de usuarios con acceso autorizado a las imágenes, con su correspondiente identificación y autenticación; a saber: Usuarios del Área de Garantía Patrimonial Corporativa, Responsables de seguridad física, responsable jurídico LOPD, Gerentes y/o jefes de tienda y responsables del Área Jurídico Laboral. Según dicho protocolo los soportes que pudieran llegar a contener imágenes identificarán la información que contienen y sólo serán accesibles por el personal autorizado al que el responsable del fichero autoriza, exclusivamente, la salida de dichos soportes, obligándose en su traslado, a adoptar medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información. Ante posibles incidencias surgidas que atenten contra la seguridad de bienes y personas, dicho protocolo establece que, dependiendo del entorno, intervendrán los diferentes responsables recurriendo, si fuera necesario, a la empresa de seguridad para que recupere las imágenes que recojan el incidente, estando obligado el Gerente/jefe de tienda/Dirección Social/RRHH a mantener al corriente de dicho incidente al Departamento Jurídico en todo momento.

En cuanto a las cuestiones asociadas a las características técnicas de la instalación y a las medidas de control de acceso al centro de control donde se realizaba la monitorización y grabación de las imágenes registradas por las cámaras, en ambos escritos se justifica la falta de respuesta al hecho de que la empresa instaladora ya no existe y a que el establecimiento comercial donde tuvieron lugar los hechos se vendió a finales de 2011 a otro operador, entregando dicha información al comprador y no quedando registrada copia de la misma por cuestiones de seguridad.

El representante legal de ambas sociedades manifiesta que los grabadores, habida cuenta del estado de la tecnología en el momento de los hechos, no soportaban el control de acceso lógico y que, teniendo en cuenta que los datos relativos a videovigilancia se correspondían con datos de nivel básico, tampoco se registraban los accesos a las grabaciones, pese a que el contrato firmado con la empresa de seguridad recogía la necesidad de *"permitir la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información"*. La conservación de las imágenes grabadas, según aclara, se hacía conforme a ley y al protocolo de videovigilancia, no superando el plazo de 30 días.

En relación a las posibles cesiones realizadas de las grabaciones registradas, el representante legal de ambas sociedades refiere, como ya se ha indicado, que no le consta que se produjese extracción alguna de las grabaciones ni comunicación a terceras partes, apuntando a la empresa responsable del servicio de seguridad como la encargada de extraer las grabaciones aunque, en el protocolo de tratamiento de la imagen, esta no figura entre la relación tasada de usuarios con acceso a los datos y el propio contrato, en la estipulación *DECIMOQUINTA* relativa a la confidencialidad recoge que *"Exclusivamente la Propiedad, en coordinación con el Contratista, o viceversa, podrá conceder, alterar o anular el acceso autorizado sobre los Sistemas de Videovigilancia"* y que *"Si en algún momento, los soportes mencionados en el apartado anterior (grabaciones en disco o cinta) salieran fuera de los locales donde se lleva a cabo la prestación del servicio, esto requerirá autorización por parte de la Propiedad"*, no habiéndose aportado ningún documento que acredite esa delegación de funciones en un tercero o que dicho acceso fuera expresamente

autorizado por CECOSA HIPERMERCADOS, S.L. como responsable del sistema. Aclara que la forma de proceder, tanto en 2011 como en la actualidad, en el caso de que sean solicitadas imágenes, es esperar al requerimiento oficial y sólo en ese momento se produce la extracción.

DÉCIMO-CUARTO: OMBUDS COMPAÑÍA DE SEGURIDAD, en correo electrónico de 19/06/2018 registrado el 21/06/2018, da respuesta a la petición de la AEPD de 30/05/2018, aportando:

1) Copia del documento identificado como "*Manual de Órdenes de Puesto*" en la oferta presentada por CASESA en el marco del concurso realizado por el GRUPO EROSKI en Diciembre de 2010 para la adjudicación del servicio de vigilancia de negocios del grupo empresarial, así como de todos aquellos manuales de procedimientos de actuación en materia de videovigilancia y protección de datos, entre ellos "*Procedimiento para el centro de control de seguridad*", "*Procedimiento para la protección de la información" y "Procedimiento de control de acceso de personas a las instalaciones*".

Se aporta copia del *"Manual Operativo del Servicio de Seguridad de* CECOSA, EROSKI HIPER y EROSKI C.P" para los servicios de seguridad que actualmente OMBUDS presta en distintos establecimientos comerciales del GRUPO EROSKI y en el que se recogen los cometidos, las órdenes y los procedimientos operativos que deben seguir los vigilantes de seguridad en el servicio prestado; es decir, qué deben hacer y cómo deben hacerlo.

Profundizando en el perfil y las características del puesto de vigilancia, de los siete cometidos recogidos relativos a "*Control de Accesos*", "*Realización de Rondas*", "*Actuación ante emergencias y alarmas*", "*Actuación ante una amenaza telefónica de bomba"*, "Actuación ante alborotos", "*Actuación ante la detección de un posible paquete o coche bomba*" y "*Colaboración con otros servicios de seguridad*", los cuales vienen definidos con extremo nivel de detalle, en el cometido nº 3 relativo a la *"Actuación ante Emergencias y Alarmas"*, en el Procedimiento Operativo nº 2 en relación con la actuación *"ante robo, hurto o roturas"* se recoge textualmente que *"A fin de evitar situaciones posteriores complicadas (como denuncias del cliente, etc.) el vigilante debe intervenir tras llegar a estar completamente seguro. Para ello, estará en contacto con el 'Centro del C.C.T.V.' averiguando si ha quedado constancia de los hechos en la grabación del Circuito Cerrado de Televisión"* y que *"el vigilante, en su intervención ante un robo o hurto debe tener en cuenta lo siguiente: (…) Informará al cliente de que, ante la evidencias disponibles, debe abonar los productos o, en su defecto, devolverlos."* lo que parece poner de manifiesto la posibilidad de acceder, por parte del personal de la empresa de seguridad, a las grabaciones de eventos registrados desde la sala de CCTV a los efectos de comprobar la posible sustracción de productos.

No obstante, dicho manual identifica el perfil de Responsable de Seguridad, como personal encargado de la dirección, supervisión y prestación de la seguridad en CECOSA HIPERMERCADOS, S.L., EROSKI HIPER y EROSKI C.P. en la figura del Gerente, haciendo repetidas referencias a las consultas, instrucciones e indicaciones dadas por el Responsable de Seguridad del establecimiento comercial en el marco de los distintos procedimientos operativos definidos en el *Manual Operativo del Servicio de Seguridad* que debían ser seguidas por los vigilantes que prestan el servicio, en clara sintonía con lo estipulado tanto en el contrato de prestación de servicios como en el protocolo de tratamiento de la imagen y el extracto del manual de seguridad ya referenciados en lo que respecta a la revisión de las

medidas de seguridad así como a la supervisión y autorización de los accesos a los sistemas de videovigilancia y la salida de soportes por parte de la Propiedad.

2) Indicar si OMBUDS COMPAÑÍA DE SEGURIDAD, S.A. mantiene en la actualidad algún contrato para la prestación de servicios de seguridad con CECOSA HIPERMERCADOS, S.L., facilitando, en caso afirmativo, copia firmada y completa del mismo.

Deberá aportarse además toda la información complementaria, ya sea elaborada por el contratista o facilitada por la propiedad, en la que se describan los procedimientos seguidos por los vigilantes de seguridad en materia de videovigilancia, el alcance exacto de sus funciones, las instrucciones recibidas y medidas de seguridad a cumplir así como la posible delegación formal de puestos internos de la Propiedad (junto con sus cometidos y responsabilidades) en personal del Contratista encargado de la prestación de los servicios de seguridad en los establecimientos comerciales, adjuntando la documentación que acredite que los vigilantes de seguridad conocen los procedimientos a seguir y han aceptado esas funciones y responsabilidades

OMBUDS COMPAÑÍA DE SEGURIDAD, S.A. manifiesta que no ha sido posible localizar en los archivos la documentación requerida ni el personal de CASESA incorporado a OMBUDS ha podido dar razón de esta.

DÉCIMO-QUINTO: Con fecha 22/06/2018, tiene entrada escrito del Secretario General de la Jefatura Central de Seguridad Ciudadana y Coordinación en respuesta a la solicitud de 7/06/2018 a la Unidad Central de Seguridad Privada. Para aclarar el alcance real de los servicios prestados en las actividades para las que CASESA contaba con autorización en mayo de 2011, se solicitó que informara los servicios concretos que quedan enmarcados en cada una de las actividades de seguridad privada identificadas en el artículo 5 de la Ley 5/2014, de 4/04, de Seguridad Privada, y en concreto en qué actividad quedan circunscritos los servicios de videovigilancia a los que se refiere el artículo 42 de la mencionada ley. En la respuesta se aclara que la actividad de *"vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos"* (art. 5.1.a de la Ley de Seguridad Privada) se corresponde con los servicios de *"vigilancia y protección"* y "*videovigilancia"* a los que hacen referencia los artículos 41 y 42 de la mencionada Ley.

Aclaran que, la prestación de servicios de videovigilancia a los que se refiere el artículo 42 y que en sus apartados 4 y 5 regulan los principios de finalidad, proporcionalidad, idoneidad e intervención mínima de la operativa de los sistemas de videovigilancia y las grabaciones que registran, puede adoptar dos modalidades: desde un centro de control ubicado en la propia instalación a vigilar, en cuyo caso la prestación sería realizada por una empresa de seguridad autorizada para la actividad de *"vigilancia y protección"*, como era el caso de CASESA, o si el sistema de CCTV está conectado a una central receptora de alarmas, la empresa prestataria del servicio debería estar autorizada para las actividades de *"vigilancia y protección"* y *"centralización de alarmas"*.

Idénticas consideraciones vienen recogidas en el contrato actualmente vigente entre CECOSA HIPERMERCADOS S.L. y OMBUDS COMPAÑÍA DE SEGURIDAD, S.A. para la prestación de servicios de seguridad, aportado tanto por la propia CECOSA como por la empresa de seguridad en escrito de respuesta de fecha 20/06/2018 al ser preguntada por esta Agencia con fecha 30/05/2018 y número de salida 144884/2018 si mantiene en la

actualidad algún contrato de prestación de servicios de seguridad con CECOSA siendo el contenido de la cláusula *DECIMOQUINTA* del contrato de 26/04/2014 suscrito entre ambas sociedades, relativa a la confidencialidad, una copia exacta de la cláusula arriba analizada que regulaba este aspecto del servicio en el contrato suscrito entre CECOSA y CASESA en febrero de 2011, con la única salvedad de que en lugar de *"a la Propiedad"* hace referencia *"al Cliente"* y el contrato actualmente vigente amplía su alcance a más empresas del grupo empresarial y entre las que se encuentra CECOSA, en lugar de circunscribirse a esta última como era el caso del contrato de diciembre de 2010 suscrito con CASESA.

El contrato de arrendamiento servicios de seguridad vigilancia de 26/04/2014 se suscribe entre EROSKI S COOP, CECOSA SL y CECOSA SLU y otros supermercados Y GASOLINERAS (se denominan parte CLIENTE) con OMBUDS que ha sido adjudicatario del concurso , tratándose de un contrato marco, siendo el objeto del mismo la prestación del servicio de vigilancia desde 1/05/2014 a 31/01/2017 en los centro comerciales EROSKI que se mencionan en ANEXO 1 siendo los medios materiales para la prestación del servicio, defensa reglamentaria y grilletes, y sin armas. El contrato regula las condiciones que han de ser aplicadas a la totalidad de los servicios ofertados por el contratista. Se expone el orden de prevalencia de los diversos documentos de la relación, contrato marco, pliego de condiciones técnicas, anexo I con servicios a prestar por contratista, normas generales, y carta presentación, actividades de prevención.

NI en el apartado obligaciones del contratista ni en el de personal empleado por contratista o incumplimiento del contrato se hace menciona labores de acceso a datos en sistemas de videovigilancia. Únicamente la cláusula 15 indica CONFIDENCIALIADAD, que "*en cumplimiento del artículo 12 de la LOPD…se determinan en el presente contrato las obligaciones derivadas del tratamiento de datos de carácter personal a los que tenga acceso el contratista en cumplimiento de su prestación*", y la 15.1 "*Datos de carácter personal*" "En aquellos casos en que el contratista directamente o a través de su empleado pudiera tener acceso a datos de carácter personal en general entendidos como los definidos en la LOPD, entre los que se encuentran los relativo a la videovigilancia y el control de acceso físico, se obliga a no aplicar ni utilizar *ni revelar con fines distintos a los que se derivan del contrato, utilizar los datos con la única finalidad de prestar los servicios encargados, Él contratista no comunicara ni permitirá el acceso a los datos de carácter personal a ningún tercero- a excepción de aquellos empleados que no puedan cumplir sus obligaciones si tener acceso a los mismos- ni divulgara publicar ni cederá ni siquiera para su conservación a otras personas*

Dicho personal laboral del contratista deberá obligarse a mantener el carácter confidencial descrito, mediante documento privado, siendo obligación del contratista informar a sus trabajadores de las obligaciones que se derivan de la normativa de protección de datos respecto del tratamiento de datos personales durante la prestación del servicio"

También se incluye la cláusula 15.2 sobre deber de secreto respecto de los datos de carácter personal del contratista, y el 15.3 "*medidas de seguridad*" que indica que el contratista se compromete a adoptar y respetar medidas organizativas y técnicas y de seguridad que el cliente de acuerdo con lo establecido en la LOPD y su reglamento de desarrollo estime necesarias para garantizar la seguridad y confidencialidad, también se establece el principio general de acceso del contratista y empleados solo a los recursos necesarios para el desarrollo de sus funciones, y a que el cliente establecerá mecanismos

para evitar que el contratista pueda acceder a recursos con derechos distintos de los autorizados, por ello el contratista se encargara de que exista una relación actualizada de usuarios y perfiles con accesos autorizados al sistema de videovigilancia que capta y almacena las imágenes que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información. Exclusivamente el cliente, en coordinación con el contratista o viceversa podrá conceder, alterar o anular el acceso autorizado sobre los sistemas de videovigilancia.

Además del citado contrato se aporta por OMBUDS copia del pliego de condiciones del servicio de vigilancia del GRUPO EROSKI de 11/02/2014 que describe los servicios de vigilancia que se pueden prestar, también para hipermercados, supermercados y tiendas del GRUPO sobre la contratación del servicio de vigilancia. No consta en la descripción de los servicios de vigilancia o en el de "*funciones*" el de acceso y manejo de imágenes de videovigilancia o encargo de tratamiento de dicho tipo de servicio. Si figura un aparado de coordinación entre personal del grupo EROSKI y la empresa de seguridad adjudicataria pero ninguna alusión a acceso a sistemas de videovigilancia.

También figura el documento de OMBUDS de 21/03/2014 "*adjuntamos nuestra oferta económica para los servicios de vigilancia y servicios auxiliares del GRUPO EROSKI*", con unos cuadros de prestación de servicios por zonas en los que no se deduce la prestación de dicho servicio.

Se aporta un manual operativo del servicio de seguridad de CECOSA; EROSKI HIPER y EROSKI CP, edición 23/07/2014 en el que se cita entre otros, el del centro comercial "*Luz del Tajo*". El manual contiene las órdenes y procedimientos que junto con la operativa profesional del personal operativo de OMUBDS permitirán llevar a cabo una adecuada actuación y relación con el personal de contacto de OMBUDS. No se contiene ninguna referencia a los sistemas de acceso a imágenes a través de sistema de videovigilancia.

DECIMO-SEXTO: Por los hechos puestos de manifiesto y derivados de la Inspección de 23/05/2018 en EROSKI, "*Centro Comercial Luz del Tajo*", a CECOSA HIPERMERCADOS SL en fecha 4/03/2019, se acordó por la directora de la AEPD:

-Iniciar procedimiento sancionador a CECOSA HIPERMERCADOS, S.L. (EROSKI, "*Centro Comercial Luz del Tajo*"), por infracción del artículo 9 de la Ley Orgánica 15/1999, de 13/12, de Protección de los Datos de Carácter Personal (en lo sucesivo LOPD), en relación con los artículos 88.1, 89.1, 91.1) .2) .3) y 93.2), 97 y 99 del Reglamento de Desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21/12 (en adelante RLOPD), y por la infracción del artículo 4.1 de la LOPD tipificada como grave en el artículo 44.3.c) de la LOPD.

-incorporar al expediente sancionador, a efectos probatorios los documentos obtenidos y generados por los Servicios de Inspección durante la fase de investigaciones; así como el informe de actuaciones previas de Inspección; todos ellos parte del expediente

-A los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1/10 y art. 127 letra b) del RLOPD, las sanciones que pudieran corresponder sin perjuicio de la tramitación del expediente serían:

a) Una multa de 100.000 € por la infracción del artículo 9 de la LOPD.

En dicha cuantía se valoró el volumen de los tratamientos efectuados en cuanto al personal que acude a sus centros comerciales es elevado y compuesto por todas las personas que acceden a los centros comerciales en los que existen dispositivos de videovigilancia 44.4.b), la vinculación de la actividad del presunto infractor con la realización de tratamientos de datos de carácter personal forma parte de su labor profesional relacionada con la venta al público 44.4.c), tanto el volumen de negocio como la actividad comercial de hipermercados a la que se dedica se sitúan en un volumen medio-alto (44.3.d) y varios elementos se suman en las faltas de las medidas de seguridad (44.4.j),

b) Una multa de 50.000 € por la infracción del artículo 4.1 de la LOPD, valorando que la mayoría de las fotografías proceden de grabaciones de un sistema de videovigilancia, y se incluyen entre otras, personas sospechosas de hurto, considerando la acción deliberada de recopilación de datos de fotografías con el fin de ser expuestas para su visionado habitual (45.4.f) aunque la denunciada tiene interés en desplegar funciones de seguridad sobre los bienes del recinto del que es titular.

DECIMO-SÉPTIMO: El acuerdo de inicio se remitió por el sistema de notificación telemática "notifica", parte del Servicio de Notificaciones Electrónicas (SNE) y Dirección Electrónica Habilitada, (DEH) de acuerdo con la Orden PRE/878/2010 y el Real Decreto 769/2017, de 28/07 por el servicio de Soporte del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, figurando un certificado en el que se significa:

-Que a través de dicho servicio se envió la notificación:
Referencia: 89444345c7ea36d96c64
Administración actuante: Agencia Española de Protección de Datos (AEPD)
Titular: CECOSA HIPERMERCADOS, S.L. - B48231351
Asunto: "ESCRITO"
con el siguiente resultado:

Fecha de puesta a disposición: 05/03/2019 17:27:28
Fecha de rechazo automático: 16/03/2019 00:00:00

El rechazo automático se produce, de forma general, tras haber transcurrido diez días naturales desde su puesta a disposición para su acceso según el párrafo 2, artículo 43, de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas. Y de forma particular, superado el plazo establecido por la Administración actuante de acuerdo con la normativa jurídica específica que sea de aplicación.

Lo que se certifica a los efectos oportunos en Madrid a 16/03/2019"

DECIMO-OCTAVO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes hechos probados:

SOBRE LAS IMÁGENES DE VIDEO DE LOS HECHOS DE 4/05/2011 EN SUPERMERCADO EROSKI VALLECAS AVENIDA PABLO NERUDA 91–97, EN MADRID

1) Con fecha de 25/04/2018, la directora de la AEPD inicia actuaciones de investigación en relación con la publicación ese mismo día, en diferentes medios de comunicación, de imágenes procedentes de las grabaciones registradas por el sistema de videovigilancia instalado en un establecimiento comercial de la cadena de supermercados EROSKI**,** Avenida Pablo Neruda 91–97, en Madrid conocido como EROSKI VALLECAS, correspondientes a hechos acaecidos el 4/05/2011. El supermercado cerró meses después de ocurridos los hechos, traspasándose a otra cadena para, finalmente, ser vendido a otro operador que es el que lo gestiona actualmente.

2) EROSKI SOCIEDAD COOPERATIVA (EROSKI SC en lo sucesivo) es la empresa matriz del grupo que da nombre a la marca comercial del hipermercado en el que tuvieron lugar los hechos el 4/05/2011. Informó que la sociedad titular del establecimiento comercial cuando tuvieron lugar los hechos era una entidad perteneciente al mismo grupo EROSKI denominada CECOSA HIPERMERCADOS SL-(CECOSA).

3) CASTELLANA SEGURIDAD, S.A.,(CASESA) era la empresa encargada de la seguridad del establecimiento en los momentos de producirse el incidente, fusionada por su socio único OMBUDS COMPAÑÍA DE SEGURIDAD, S.A., (OMBUDS) desde 26/02/2018. Realizada visita de Inspección el 27/04/2018 a la sede social de OMBUDS, se manifestó:

3.1) No les consta que agentes de Policía se personaran en el establecimiento comercial y solicitaran copia de las grabaciones en relación con la incidencia acaecida.

3.2) El servicio de seguridad que prestaba CASESA en el supermercado era de mera vigilancia, sin acceso a los sistemas de videovigilancia, y ello figuraba en el contrato de "*arrendamiento servicios de seguridad vigilancia*" de 14/02/2011 que aporta. En dicho contrato celebrado entre CASESA y CECOSA HIPERMERCADOS SL (Compañía que explota una amplia red de establecimientos comerciales y que dispone tanto de aparcamientos, oficinas, almacenes etc. para el desarrollo de la actividad que le es propia. SE acompaña una relación de "hipermercados" del grupo EROSKI en el Anexo 1. Se contrata el servicio de vigilancia, con los medios de "*defensa reglamentaria y grilletes*", y sus condiciones se aplican a "la totalidad de los servicios o trabajos que habiendo sido ofertados por parte del contratista a la propiedad, hayan sido expresamente aceptados".

3.3) Existe una cláusula en el contrato de 14/02/2011 (clausula 15) del tenor:

-15 "*confidencialidad*" "*en cumplimiento del artículo 12 de la LOPD… se determinan las obligaciones derivadas del tratamiento de datos a los que tenga acceso el contratista en cumplimiento de su prestación*"

-15.1"*datos de carácter personal*" en *"los casos en que el contratista o sus empleados pudieran tener acceso a datos de carácter personal, entre los que se encuentran los de videovigilancia y el control de acceso físico se obliga a no aplicar ni utilizar ni revelar con fines distintos a los que se derivan del contrato, utilizar los datos con la única finalidad de prestar los servicios encargados, y que el personal laboral deberá mantener el carácter confidencial, siendo obligación del contratista informar a sus trabajadores de las obligaciones que derivan de la normativa de protección de datos respecto del tratamiento de datos personales durante la prestación del servicio*" También se establece el deber del secreto para el contratista y sus empleados.

-15.3 establece que el contratista se compromete a adoptar las medidas de seguridad que el titular estime necesarias de acuerdo con lo establecido en la LOPD para garantizar la confidencialidad y seguridad de los datos, siendo el nivel de seguridad de los datos derivados de la prestación de servicios, el básico, Se indica que el contratista y sus empleados tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. Y que "*el contratista se encargara de que exista una relación actualizada de usuarios y perfiles con accesos autorizados al sistema de videovigilancia que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información*". "*Exclusivamente la propiedad en coordinación con el contratista o viceversa, podrá conceder, alterar o anular el acceso autorizado sobre los sistemas de videovigilancia*." "*Se prevé también que si los soportes y documentos que contengan datos de carácter personal, así como las grabaciones en disco o cinta salieran de los locales donde se lleva a cabo la prestación de servicios, requerirá autorización por parte de la propiedad*" y que "*El contratista deberá notificar a la propiedad las incidencias que afecten a los datos de carácter temporal. Asimismo, establecerá un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso detectado*…"

Se establecía pues, un deber de confidencialidad de los datos que hipotéticamente pudiera llegar a conocer el personal de CASESA en el desempeño de sus labores de videovigilancia y control de acceso físico, si bien no se celebró contrato entre las partes que especificara y regulara los accesos por los vigilantes de seguridad de CASESA al sistema de videovigilancia ni se especificara a efectos del artículo 12 de la LOPD dichos accesos y medidas.

Señala OMBUDS que la citada clausula 15 está redactada de modo genérico

3.4) El personal de seguridad "*no tenía acceso al sistema de videograbación, al que solo podía acceder el Gerente del supermercado*". El vigilante de seguridad de CASESA que prestaba servicio el día de los hechos, relató a la Policía que los datos personales de videovigilancia a los que accedía eran los de los monitores, en tiempo real y así fue como presenció el hurto relacionado con los hechos que gestionó.

El Inspector de zona de CASESA adscrito al citado supermercado, que anteriormente desempeño el cargo de jefe de seguridad del establecimiento, manifestó que la persona autorizada para tratar las imágenes era el "*Gerente del centro*", disponiendo en su despacho de un ordenador con el programa para extraer las imágenes, y caso de urgencia, también las podían extraer otras personas como la jefa de personal y el encargado del bazar. Indica que el despacho de Gerente estaba cerrado con llave de la que disponía además del gerente, la jefa de recursos humanos. Añade que en caso de extraerse imágenes, eran entregadas por quien las había obtenido al servicio de seguridad, para que estos le dieran el tramite oportuno, si bien no tiene conocimiento de que las del hecho aquí relacionado fuesen gestionadas por el personal de seguridad.

4) EROSKI SOCIEDAD COOPERATIVA manifestó que CASESA era la encargada de prestar los servicios, con acceso a las grabaciones dentro del centro, aportando copia del

citado contrato "*marco*" de 14/02/2011, del cual como se comprueba no se deduce tal manifestación. También afirma que la empresa encargada de la instalación del sistema de videovigilancia se denominaba EKINTZA, ya extinguida.

5) EROSKI señala que con la empresa SABICO se contrató el servicio de Central Receptora de Alarmas (CRA) con capacidad de acceso remoto a las grabaciones del sistema y que la finalidad de la instalación del sistema de videovigilancia en el supermercado fue la de garantizar la seguridad de los bienes y personas.

Según manifestó Eroski, existía en el citado supermercado un protocolo de videovigilancia- ANEXO 4 y una nota informativa videovigilancia 2009 y 2010 y nota ejercicio de derechos 2013

6) En las actuaciones de inspección no ha sido posible obtener copia ni reseña inventariada de las imágenes del sistema de videovigilancia que contienen los hechos acontecidos el 4/05/2011 y que se reprodujeron en varios medios de comunicación y televisión

7) En las actuaciones de inspección, EROSKI manifestó que: *en 2011 en el hipermercado en el que se produjeron los hechos investigados de 4/05/2011:*

- los sistemas eran videograbadores que no soportaban control de acceso lógico, y el modelo no permitía el acceso con clave.

- *No se* realizaban auditorías sobre el sistema de grabaciones de imágenes, a efectos de verificar por ejemplo los accesos y sus tipos, ni se *registraban los accesos a las grabaciones.*

-No existía sistema de registro de soportes de entrada y salida

- A la cuestión de si el acceso a los videograbadores se realizaba con claves de usuario y contraseña, EROSKI manifestó que entiende en 2011 los accesos no se realizaban con clave, no se registraban los accesos a las grabaciones, ni se realizaban auditorías ni existía registro de entradas y salidas de soportes indicando que las imágenes se conservaban por no más de 30 días.

8) La Dirección General de la Policía Indica en relación con los hechos que no consta ni en los registros de la Sala 091 ni en el libro oficial de telefonemas de la Comisaría de Distrito de Puente de Vallecas ningún asiento relativo a la recepción de una llamada realizada desde el establecimiento comercial en relación con el incidente, así como tampoco consta ningún parte de servicio sobre la intervención de ningún indicativo de dicha dependencia policial

9) CECOSA en su respuesta de 14/06/2018 no fue capaz de identificar al personal del supermercado que a la fecha de los hechos accedía a las imágenes del sistema, ni del personal interno o externo que podía acceder a las grabaciones del sistema de videovigilancia ni soporte documental de atribución de funciones y responsabilidades en la materia

10) CECOSA en su repuesta de 14/06/2018 coincide en informar que la instalación del supermercado se realizó por EKINTZA ya extinguida y en cuanto a las cuestiones asociadas a las características técnicas de la instalación y a las medidas de control de acceso al centro de control donde se realizaba la monitorización y grabación de las imágenes registradas por las cámaras, justifican su falta de respuesta al hecho de que la empresa instaladora ya no existe y a que el establecimiento comercial donde tuvieron lugar los hechos se vendió a finales de 2011 a otro operador, entregando dicha información al comprador y no quedando registrada copia de la misma por cuestiones de seguridad.

11) CECOSA ratifica que el contrato de seguridad con CASESA era un contrato tipo, marco, que regula condiciones contractuales y técnicas del servicio prestado, aplicable a los hipermercados del GRUPO

12) CECOSA reitera que para acceder a los datos no existía control de acceso lógico, no se registraban los accesos a las grabaciones

CECOSA manifestó, que no le consta que se produjese extracción alguna de las grabaciones ni comunicación a terceras partes, apuntando a la empresa responsable del servicio de seguridad como la encargada de extraer las grabaciones aunque, en el protocolo de tratamiento de la imagen, esta no figura entre la relación tasada de usuarios con acceso a los datos y el propio contrato, en la estipulación *DECIMOQUINTA* relativa a la confidencialidad recoge que *"Exclusivamente la Propiedad, en coordinación con el Contratista, o viceversa, podrá conceder, alterar o anular el acceso autorizado sobre los Sistemas de Videovigilancia"* y que *"Si en algún momento, los soportes mencionados en el apartado anterior (grabaciones en disco o cinta) salieran fuera de los locales donde se lleva a cabo la prestación del servicio, esto requerirá autorización por parte de la Propiedad"*, no habiéndose aportado ningún documento que acredite esa delegación de funciones en un tercero o que dicho acceso fuera expresamente autorizado por CECOSA HIPERMERCADOS, S.L. como responsable del sistema.

SOBRE EL HIPERMERCADO DE EROSKI GESTIONADO POR CECOSA HIPERMERCADOS, S.L., SITUADO EN EL "*CENTRO COMERCIAL LUZ DEL TAJO*", TOLEDO.

1) El 23/05/2018, se realizó una visita de inspección por la AEPD en el hipermercado de EROSKI titularidad de CECOSA HIPERMERCADOS, S.L., situado dentro del "*Centro Comercial Luz del Tajo*", Toledo para verificar el sistema de videovigilancia.

2) Por manifestaciones de CECOSA se conoce que el sistema fue instalado en 2004 por INGECOM que también efectúa labores de mantenimiento. INGECOM solo tiene acceso a grabaciones previo requerimiento del departamento de seguridad de su cliente, prestando el servicio de extracción técnica y entregando a la persona designada por su cliente el

soporte externo con las imágenes. Manifiestan que para el modo grabación se necesita usuario y contraseña, pudiendo estar habilitados para realizar visionado directo de las cámaras, reproducción de imágenes previamente registradas, manifestando que el acceso a los grabadores además de localmente a través de los monitores directamente conectados se puede realizar desde la red local de EROSKI.

3) Según manifestó el Gerente del supermercado, la finalidad del sistema es la de prevenir hurtos y robos de productos teniendo además contratado servicios de seguridad y vigilancia con la empresa OMBUDS, a través de un jefe de equipo y un vigilante de seguridad, encargados de cubrir los turnos de mañana y tarde. El contrato de vigilancia con OMBUDS firmado el 26/04/2014 figura suscrito por distintas entidades integrantes del GRUPO EROSKI entre las que figuran hipermercados, supermercados y gasolineras del GRUPO EROSKI, entre otras también CECOSA HIPERMERCADOS , y responde a un tipo de contrato marco que regula las condiciones contractuales y técnicas del servicio prestado resultado de su adjudicación en forma de concurso. El contenido del contrato es similar al de 14/02/2011 entre CECOSA HIPERMERCADOS y CASESA.

El objeto del contrato de 26/04/2014 es la vigilancia que se desarrollará en centros comerciales del grupo EROSKI contenidos en el ANEXO 1. Como medios materiales para la prestación del servicio no consta la videovigilancia. Aunque se prevé una cláusula general (15) de confidencialidad en cumplimiento del artículo 12 de la LOPD en la que se indica que " *se determinan las obligaciones derivadas del tratamiento de datos a los que tenga acceso el contratista en cumplimiento de su prestación*", se señala a continuación en el 15.1 que en los *casos en que el contratista directamente o a través de sus empleados pudiera tener acceso a datos de carácter personal, entre los que se encuentran los relativos a la videovigilancia y el control de acceso físico, se obliga a: "No aplicar ni utilizar ni revelar los datos de carácter personal con fines distintos a los que se derivan del presente contrato, con la exclusiva finalidad de prestar los servicios encargados, que no comunicara ni permitirá el acceso a ningún tercero y que dicho personal laboral del contratista Deberá obligarse a mantener el carácter confidencial siendo obligación del contratista informar a sus trabajadores de las obligaciones que se derivan de la normativa de protección de datos respecto del tratamiento de los datos personales durante la prestación del servicio"*.15.2 "*El contratista se compromete a mantener el deber de secreto respecto a los datos de carácter personal. Obligación que subsistirá aun después de finalizar su relación contractual*. "En el artículo 15.3 se indica que "*El contratista se compromete a adoptar y respetar las medidas organizativas técnicas y de seguridad que el cliente de acuerdo con lo establecido en la LOPD y su reglamento de desarrollo estime necesarias para garantizar la seguridad y confidencialidad de los datos de carácter personal impidiendo cualquier alteración. El contratista y sus empleados tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. El cliente establecerá mecanismos para evitar que el contratista pueda acceder a recursos con derechos distintos de los autorizados, por ello el contratista se encargara de que exista una relación actualizada de usuarios y perfiles con accesos autorizados al sistema de videovigilancia que capta y almacena las imágenes que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información Exclusivamente el cliente, en coordinación con el contratista o viceversa, podrá conceder , alterar o anular el acceso autorizado sobre los sistemas de videovigilancia. Los soportes y documentos en general que contengan datos de*

carácter persona así como las grabaciones en disco o cinta, en particular deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por personal autorizado para ello. Si en el algún momento los soportes mencionados en el apartado anterior salieran de los locales donde se lleva a cabo la prestación el servicio, esto requerirá autorización por parte del cliente. " Pese a todo este contenido, no se acredita la celebración concreta y especifica de un contrato especifico de control y acceso a datos de videovigilancia por parte de OMBUDS a las imágenes que en el centro comercial se puedan recoger y registrar.

4) El personal de seguridad de OMBUDS está presente durante el día pero una vez cierra el establecimiento el servicio de vigilancia en horario nocturno es cubierto de forma remota por la empresa SABICO que realiza las funciones de CRA (Central Receptora de Alarmas)

5) El sistema de videovigilancia se compone de un total de 58 cámaras ninguna de las cuales realiza grabación de sonido, de ellas, 10 son de tipo domo con zoom y capacidad de movimiento y el resto fijas, repartidas por toda la superficie del hipermercado.

6) Las imágenes registradas por las cámaras se visualizan desde monitores ubicados:

- en el despacho del Gerente,

-en el puesto de control o pódium situado a la entrada del hipermercado,

-en el centro de control que es donde además se localiza el sistema de grabación compuesto por tres grabadores de 16 canales ,capaces de almacenar las grabaciones de un total de 48 cámaras.

Indica el Gerente de Eroski, que a la visualización de las imágenes tienen acceso el Gerente y el personal de seguridad.

7) Indica el Gerente que en el establecimiento existe una zona de acceso restringido solamente al personal en la que se sitúa el centro de control de seguridad, el cuarto de intervención, el acceso a la zona de caja central y mostrador de atención al cliente. El acceso a dicha zona se realiza a través de una puerta que está permanentemente cerrada y solamente dispone de la llave el jefe de equipo de la empresa que presta servicios de seguridad. También es posible la apertura de la puerta mediante un pulsador que se encuentra en la caja central. Una vez en el interior de la zona de acceso restringido, todos

los cuartos se encuentran con las puertas abiertas, incluido el centro de control. Se comprueba que en el centro de control existen cinco monitores en los que se reproducen las imágenes en tiempo real. Se comprueba que existen además tres grabadores.

7) Se verifica durante la visita de inspección , que el acceso a las imágenes grabadas se realiza a través del software del grabador, siendo necesaria la identificación y autenticación mediante la introducción de un código de usuario y una contraseña. Se manifiesta por el Gerente que existen cuatro perfiles siendo dos de ellos administrador, un usuario gerente, un usuario EROSKI y un usuario seguridad. Manifiesta el Gerente que "*El jefe de equipo de la empresa de seguridad accede al sistema tanto con el perfil gerente como con el perfil seguridad*" y que "*Cuando el gerente necesita acceso a las imágenes grabadas se lo requiere al personal de la empresa seguridad que es el que realiza el acceso o, en su caso, la extracción*". Se accede por Inspección al software de gestión con el perfil de GERENTE y se comprueba que en los tres grabadores las imágenes más antiguas conservadas corresponden al día 17/05/2018. Se comprueba que seleccionando una cámara y un intervalo de fechas, el software de gestión del grabador permite la extracción de las imágenes seleccionadas a un soporte externo.

Los Inspectores comprueban que sobre uno de los monitores hay pegado un pos-it que contiene el código de usuario administrador y la contraseña. Se solicita el acceso con dichos códigos comprobando que permiten el acceso al software de gestión de grabaciones.

8) Manifiesta el Gerente que, cuando el necesita acceder a las imágenes de alguna de las grabaciones del sistema, se lo requiere al personal de la empresa de seguridad que es el que realiza el acceso y, en su caso, la extracción de las imágenes, a través del puerto USB con el que cuentan los grabadores, a un soporte externo, seleccionando para ello, según demostración realizada por el Jefe de equipo de seguridad, la cámara que registró las imágenes solicitadas y el intervalo de fechas requerido. -Solicitado que se aporten procedimientos documentados en el marco de las tareas de videovigilancia,

9) El Gerente manifestó que "*no existe ningún protocolo documentado, ni de los usuarios y perfiles de acceso así como ningún documento firmado en el que se recojan las responsabilidades y aceptación de funciones del personal*", aportando como única información escrita y documentada un manual de EROSKI denominado *"Manual de Orientación Profesional para Vigilantes de Seguridad"* que regula los procedimientos de actuación de los vigilantes de seguridad ante situaciones conflictivas con clientes y empleados pero en el que no se hace ninguna referencia a los procedimientos operativos, las funciones, cometidos y responsabilidades del personal de la empresa de seguridad en materia de videovigilancia.

10) Durante la inspección de CECOSA el 23/05/2018, dentro del cuarto destinado a centro de control en una de sus paredes se exhiben, en modo mosaico, numerosas fotografías de personas sospechosas de cometer ilícitos, algunas de las cuales datan del año 2005, según muestra incorporada como prueba al expediente. Según las aclaraciones facilitadas por el

Gerente del establecimiento, proceden de la Policía, de otros centros comerciales e incluso de otros operadores y llegan normalmente por email. También proceden del sistema de grabación del propio establecimiento, si bien como en el centro de control no hay ordenador ni impresora, son extraídas a un dispositivo externo tipo USB y se imprimen en alguno de los equipos utilizados por el personal de *EROSKI*. Se recogen fotografías de la mencionada pared en la que figuran unas 15 más o menos. Los individuos aparecen en el interior de hipermercados o del centro comercial, algunas con anotaciones manuales, otras parecen extraídas de sistemas de videovigilancia, observándose que en una de ellas aparece un individuo con su huella dactilar.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37.g) en relación con el artículo 36 de la LOPD.

II

En cuanto a la notificación del acuerdo de inicio, se cursó a través de la plataforma "*notifica*"

La LPCAP añade en su artículo 43:"*Práctica de las notificaciones a través de medios electrónicos*":

1. Las notificaciones por medios electrónicos se practicarán mediante comparecencia en la sede electrónica de la Administración u Organismo actuante, a través de la dirección electrónica habilitada única o mediante ambos sistemas, según disponga cada Administración u Organismo.

A los efectos previstos en este artículo, se entiende por comparecencia en la sede electrónica, el acceso por el interesado o su representante debidamente identificado al contenido de la notificación.

2. Las notificaciones por medios electrónicos se entenderán practicadas en el momento en que se produzca el acceso a su contenido.

Cuando la notificación por medios electrónicos sea de carácter obligatorio, o haya sido expresamente elegida por el interesado, se entenderá rechazada cuando hayan transcurrido diez días naturales desde la puesta a disposición de la notificación sin que se acceda a su contenido.

3. Se entenderá cumplida la obligación a la que se refiere el artículo 40.4 con la puesta a disposición de la notificación en la sede electrónica de la Administración u Organismo actuante o en la dirección electrónica habilitada única.

4. Los interesados podrán acceder a las notificaciones desde el Punto de Acceso General

electrónico de la Administración, que funcionará como un portal de acceso.

El artículo 14 de la misma norma indica: ”*Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas*“:

2. En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:

a) Las personas jurídicas.”

Y se concreta en el artículo 41” *Condiciones generales para la práctica de las notificaciones “1. Las notificaciones se practicarán preferentemente por medios electrónicos y, en todo caso, cuando el interesado resulte obligado a recibirlas por esta vía*.”

Como consecuencia, la notificación del acuerdo se entiende producida con todos los efectos jurídicos.

Si bien en el acuerdo de inicio se indicaba que “*si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP)*.”, se considera conveniente remitir la propuesta por a efectos de su puesta de manifiesto y conocimiento.

III

Previamente a analizar la imputación de los hechos, conviene determinar el papel que la empresa de seguridad, y los empleados dedicados a la vigilancia, de la empresa OMBUDS, antes CASESA tienen en los hipermercados donde se producen los hechos en 2011 y después en la inspección llevada a cabo en el Centro Comercial Luz del Tajo.

Como conceptos previos, será responsable del fichero o del tratamiento, conforme al artículo 3 d) de la LOPD, “*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*”. Por su parte, es encargado del tratamiento, según el artículo 3 g), “*la persona física o jurídica, autoridad, servicio o cualquier otro organismo que, solo o juntamente con otros, trate datos personales por cuenta del responsable del tratamiento*”.

En cuanto a los requisitos formales de este tipo de contratos, el artículo 12.2 de la LOPD impone que “*la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas”.*

El hecho de que la relación derivada del contrato sea la existente entre un responsable y un encargado del tratamiento implicará que al término de la relación sea

aplicable lo establecido en el artículo 12.3 de la LOPD, de forma que "*una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".*

El incumplimiento de esta previsión llevará aparejada la consecuencia, prevista en el artículo 12.4 de la LOPD, de que *"En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".*

Otra consecuencia se deriva a sensu contrario de la falta de los elementos necesarios para la existencia del encargo, previstas en el párrafo 12.1 de la LOD *"No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento*.", es decir, si no existe el citado contrato como es en ambos casos, se podría estar produciendo un tratamiento de datos sin consentimiento por parte del destinatario de los datos, y un tratamiento en forma de cesión por parte del cedente.

Lo importante para delimitar los conceptos de responsable y encargado del tratamiento no resultan ser la causa que motiva el tratamiento de los mismos, sino la esfera de dirección, control u ordenación que el responsable pueda ejercer sobre el tratamiento de los datos de carácter personal que obran en su poder en virtud de aquella causa y que estaría enteramente vedado al encargado del tratamiento.

La figura del encargado del tratamiento es esencial en la legislación de protección de datos, de modo que el encargado, junto con el responsable del tratamiento, debe adoptar medidas necesarias que garanticen la seguridad de los datos (art. 9 LOPD) y será en consecuencia responsable a efectos sancionadores (art. 43 LOPD).

Para que la relación entre responsable y encargado del tratamiento pueda ser calificada como tal, es preciso que se cumplan los requisitos expresados en el artículo 12 de la LOPD.

En primer lugar, es preciso que el acceso a los datos por el tercero se efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero, y que dicha relación de servicios se encuentre contractualmente establecida, tal y como desarrolla el artículo 20 del Real Decreto 1720/2007, de 21/12, por el que se aprueba el Reglamento de desarrollo de la LOPD (RLOPD); es decir, el contrato deberá ser concertado entre el responsable y el encargado del tratamiento.

En este sentido, la propia Ley prevé un contenido mínimo del contrato entre las partes en el que deben constar una serie de estipulaciones necesarias, a saber, seguir las instrucciones del responsable del tratamiento, no utilizar los datos para un fin distinto, no comunicarlos a otras personas (artículo 12.2 párrafo primero), estipular las medidas de seguridad del artículo 9 (artículo 12.2 párrafo segundo), y cumplida la prestación destruir los datos o proceder a su devolución al responsable del tratamiento (artículo 12.3).

Pues bien, en los dos casos examinados en este supuesto, video de EROSKI Vallecas

de 4/11/2011 y visita de Inspección Centro comercial Luz del Tajo, supermercado de CECOSA, se puede concluir:

a) Los contratos marcos de prestación del servicio de vigilancia adjudicados a CASESA y a OMBUDS, muy similares en su referencia a datos personales señalaban que el servicio era de vigilancia, en el segundo contrato para varios centros y dependencias pertenecientes a la rama EROSKI, en el primero para distintos supermercados de CECOSA.

b) Después de los contratos marco no se celebró con la adjudicataria contrato concreto que se ajustara a los extremos del artículo 12 de la LOPD en materia de videovigilancia ni a nivel general, ni a nivel particular, centro a centro. Por tanto, y así se acredita, no existen protocolos de actuación y manejo de datos resultantes del acceso al sistema de videovigilancia celebrado entre las partes, titular del supermercado y OMBUDS, ni los empleados son conocedores y han sido informados específicamente de sus obligaciones al respecto en cuanto a manejo o deberes concretos resultantes de sus accesos al sistema.

La consecuencia es que CECOSA HIPERMERCADOS es la responsable de los datos de videovigilancia y carece de soporte legitimo para ceder dichos datos a los vigilantes del establecimiento, sea a nivel de acceso a las mismas, para grabar o gestionar extracciones del sistema de videovigilancia.

IV

Se imputa en el presente procedimiento a CECOSA HIPERMERCADOS una infracción del artículo 9 de la LOPD, que dispone:

"*1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

El citado artículo 9 de la LOPD establece el "*principio de seguridad de los datos*" imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el "acceso no autorizado" por parte de terceros.

La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se refiere a normas reglamentarias.

El Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21/12, (RLOPD) LOPD, en relación con las medidas de seguridad de los ficheros establece:

artículo 88.1,

"*El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.*

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos."

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo."

Artículo 89

"*1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.*

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento."

En la visita de Inspección al centro comercial, CECOSA acredita carecer de documento alguno que protocolice y se ocupe del tratamiento de las tareas de videovigilancia, el Gerente y el jefe de equipo de seguridad refieren que "*no existe ningún protocolo documentado, ni de los usuarios y perfiles de acceso así como ningún documento firmado en el que se recojan las responsabilidades y aceptación de funciones del personal*"

Artículo 91 Control de acceso

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."

Artículo 93 Identificación y autenticación

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible."

Artículo 99

"Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información."

Durante la inspección se verifica que el acceso al espacio de control de seguridad donde se hallan los grabadores y monitores es accesible a cualquier persona pulsando un timbre y las puertas se hallan abiertas, vulnerándose esta medida

En cuanto se acredita que el acceso al sistema de grabación requiere la introducción de un usuario y contraseña, estando definidos cuatro perfiles: uno de ellos para un usuario seguridad, se indicó que "El jefe de equipo de la empresa de seguridad accede al sistema tanto con el perfil gerente como con el perfil seguridad. Cuando el gerente necesita acceso a las imágenes grabadas se lo requiere al personal de la empresa de seguridad que es el que realiza el acceso o en su caso la extracción". Sobre ello cabe significar que no existe contrato de encargado de tratamiento con OMBUDS y los accesos de los empleados de esta entidad no pueden articularse en dicho acceso. Tampoco es correcto que una persona acceda con dos usuarios, el que podría tener como propio el jefe de equipo de la empresa de seguridad como el que le es prestado por el Gerente y que no tiene por qué conocer.

En el mismo sentido, la anotación en un documento en papel con las claves para el acceso como se reveló en la inspección supone una infracción de medidas de seguridad.

Los niveles de seguridad de tratamientos y ficheros de datos personales a considerar: básico, medio y alto previstos en el RLOPD deben surgir, a raíz de una previa valoración de los riesgos, qué medidas de seguridad son necesarias en cada caso. Por lo tanto, con carácter previo al tratamiento de datos habrá que llevar a cabo este análisis de tipos de datos, con el nuevo RGPD serían nivel y probabilidad de riesgos, para establecer las medidas técnicas y organizativas a fin de garantizar un nivel de seguridad adecuado.

En este sentido, hacer saber que, si bien el esquema de medidas de seguridad previsto en el RLOPD no seguirá siendo válido de forma automática a partir del RGPD, en algunos supuestos se podrán seguir aplicando estas mismas medidas si del análisis de riesgos previo se concluye que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado al caso concreto, pero puede ser necesario completarlas con medidas adicionales.

V

La infracción del artículo 9 de la LOPD se tipifica como grave en el artículo 44.3.h) que indica: "*Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen*."

VI

Por disponer de fotografías de personas sospechosas de hurto (la más antigua de 2005) se imputa a CECOSA HIPERMERCADOS SL una infracción del artículo 4.1 que indica*: "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."

Los datos de personas relacionadas con investigación de hurtos pueden ser recogidos y tratados por las Fuerzas y Cuerpos de Seguridad del Estado que con ciertos requisitos, y entre otras, tienen atribuida dicha función, pasando a integrarse en ficheros policiales. Sobre dichos datos no se contempla su cesión o uso por parte de una entidad privada. Asimismo, imágenes previas del autor de un hurto obtenidas en el mismo supermercado o procedente de otro no deben ser objeto de recopilación almacenamiento o listado para por ejemplo evitar que accedan al establecimiento público. Ello quiebra no solo la obligación de eliminar las imágenes sino que se recogen datos sin habilitación alguna.

La infracción se tipifica como grave en el artículo 44.3.c) que señala: "*Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave*."

VII

A efectos de una evaluación de las cuantías de las sanciones a imponer se reproducen el artículo 45.2. 4 y 5 de la LOPD, que señalan:

"*2. Las infracciones graves serán sancionadas con multa de 40.001 € a 300.000 €* "

"*4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:*

a) El carácter continuado de la infracción.

b) El volumen de los tratamientos efectuados.

c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

d) El volumen de negocio o actividad del infractor.

e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f) El grado de intencionalidad.

g) La reincidencia por comisión de infracciones de la misma naturaleza.

h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.

i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida

y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente."

En cuanto a la infracción del artículo 9 por CECOSA HIPERMERCADOS SL, se consideran:

-El volumen de los tratamientos efectuados en cuanto al personal que acude a sus centros comerciales es el compuesto por todas las personas que acceden 45.4.b)

-La vinculación de la actividad del presunto infractor con la realización de tratamientos de datos de carácter personal forma parte de su labor profesional habitual relacionada con la venta al público 45.4.c).

-Tanto el volumen de negocio como la actividad comercial de hipermercados a la que se dedica se sitúan en un volumen medio-alto (45.4.d).

-Varios elementos se suman en las faltas de las medidas de seguridad (45.4.j) cobrando especial relevancia la falta de medidas en cuanto al tratamiento de datos plasmada en un documento de seguridad y el conocimiento y asignación de claves de usuario establecidas. Estas circunstancias acumuladas suponen una sanción por una cuantía de 100.000 euros.

En cuanto a la infracción del artículo 4.1 de la LOPD por CECOSA HIPERMERCADOS SL, se consideran:

La mayoría de las fotografías proceden de grabaciones de un sistema de videovigilancia, y se incluyen entre otras, personas sospechosas de hurto. (45.4.j)

Considerando la acción deliberada de recopilación de datos de fotografías con el fin de ser expuestas para su visionado habitual (45.4.f) aunque la denunciada tiene interés en desplegar funciones de seguridad sobre los bienes del recinto del que es titular, se acuerda la imposición de una multa de 50.000 euros.

Vistos los preceptos citados y demás de general aplicación,

la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a la entidad **CECOSA HIPERMERCADOS, S.L.,** una multa de **100.000 euros** por una infracción del artículo 9 de la LOPD, en relación con los artículos 88.1, 89, 91, 93 y 99 del RLOPD, tipificada como grave en el artículo 44.3.h) de la LOPD, de conformidad con el artículo 45.2), 45.4.b), 45.4. c), 45.4. d) y 45.4.j) de la LOPD.

SEGUNDO: IMPONER a la entidad **CECOSA HIPERMERCADOS, S.L.,** una multa de **50.000 euros** por una infracción del artículo 4.1 de la LOPD, tipificada como grave en el artículo 44.3.c) de la LOPD, de conformidad con lo establecido en el artículo 45.2) y 45.4.f) y 45.4.j) de la citada LOPD.

TERCERO: NOTIFICAR la presente resolución a **CECOSA HIPERMERCADOS, S.L.**

CUARTO**:** Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea ejecutiva la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas, (LPACAP) en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29/07, en relación con el art. 62 de la Ley 58/2003, de 17/12, mediante su ingreso en la cuenta restringida nº ES00 0000 0000 0000 0000 0000, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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 30/12, 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 22/12, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21/12.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la LPACAP, 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 13/07, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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