

- **Procedimiento N°: PS/00382/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: Con fecha 6 de julio de 2020 tiene entrada en la Agencia Española de Protección de Datos (AEPD) un escrito remitido por D. ^a **A.A.A.** (*en lo sucesivo, la reclamante) mediante el que formula una reclamación contra A CULLER DE TERESA, S.L., con NIF B27862747 (en adelante, el reclamado) por una presunta vulneración de la normativa de protección de datos de carácter personal relacionada con el sistema de videovigilancia que tiene instalado en su local de negocio.

El motivo en el que funda la reclamación es la existencia de tres videocámaras en el muro exterior del local del reclamado —***DIRECCION.1 - que, según manifiesta, “se orientan única y exclusivamente a la vía pública (...) La vía pública que abarcan incluye aceras, la vía con tráfico rodado (***DIRECCION.1) e incluso la entrada a portales de edificios”. Añade que “no consta panel informativo alguno de la instalación de las cámaras de videovigilancia, ni información alguna de empresa responsable del tratamiento de datos”.

Anexo a la reclamación se ha aportado un reportaje fotográfico integrado por cinco fotografías de las que se obtiene la siguiente información:

- Tres fotografías versan sobre una misma videocámara: negra, de formato esférico e instalada paralela al suelo sujeta por un extremo al perfil de una ventana; perfil que es también paralelo al suelo.
En la primera fotografía se aprecia el muro exterior de un edificio sobre el que hay una gran ventana vertical de perfiles metálicos en color negro. La fotografía está captada desde el exterior del edificio. El muro exterior, en su confluencia con el extremo superior de la ventana, tiene un entrante de varios centímetros en dirección al interior del edificio, es horizontal y, por tanto, paralelo al suelo. Al entrante del muro, que está revestido, como el resto, de piedra gris, le siguen unos centímetros que no están revestidos de piedra sino cubiertos por el perfil exterior de la ventana. Sobre él está instalada la videocámara. La posición de la cámara es, por tanto, paralela al suelo y perpendicular al muro y a la ventana. Las fotografías 2 y 3 captan prácticamente la misma imagen. No obstante, es la fotografía 3 la que confirma la posición de la cámara. El modelo de cámara no permite saber por su aspecto externo hacia dónde está enfocada.
- Las fotografías 4 y 5 ofrecen la imagen de dos videocámaras de color gris instaladas sobre un soporte que es perpendicular al muro exterior de piedra. Las cámaras enfocan a la derecha y a la izquierda del muro en un plano casi paralelo a él. El objetivo de la cámara respecto al muro tiene un ángulo algo menor de 45° pues parece estar girada unos grados en dirección al muro. Debajo de las cámaras, sobre el muro, existe una gran ventana que se extiende en posición horizontal. Se intuye que justo enfrente de la ventana hay

varias casas porque la fotografía capta el reflejo de las casas sobre el cristal de la ventana.

Teniendo en cuenta el ángulo de visión de las cámaras, no pueden captar las viviendas reflejadas en el cristal pues para ello el ángulo del objetivo debería de ser otro, perpendicular al muro. No obstante, resulta evidente que, por el ángulo que tienen las dos cámaras en relación con el muro del edificio, están captando vía pública, en definitiva, elementos externos ajenos al inmueble que pretenden proteger. Las fotografías no nos muestran qué elementos físicos quedan al alcance de las dos videocámaras, pero, por su posición, la zona que abarca la captación de imágenes excede claramente de la permitida.

- En ninguna de las cinco fotografías remitidas a la AEPD consta la existencia de un cartel informativo de zona videovigilada.

SEGUNDO: Con carácter previo a la admisión a trámite de esta reclamación, en el marco del E/6057/2020, de acuerdo con lo establecido en el artículo 65.4 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD), la AEPD dio traslado de ella al reclamado.

El certificado expedido por la FNMT que obra en el expediente acredita que el 17/07/2020 la Subdirección de Inspección dirigió un escrito al reclamado con el que le daba traslado de la reclamación. El envío se notificó electrónicamente al reclamado el 17/07/2020 y consta aceptada la notificación el 21/07/2020. El reclamado no respondió a la solicitud informativa.

La Directora de la AEPD acordó admitir a trámite la presente reclamación en fecha 13/10/2020. El acuerdo de admisión a trámite se notificó a la reclamante por medios electrónicos el 13/10/2020. El certificado emitido por la FNMT que obra en el expediente acredita que la notificación fue aceptada por la reclamante el 14/10/2020.

TERCERO: Con fecha 8 de febrero de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del Artículo 5.1.c) del RGPD, Artículo 13 del RGPD, tipificada en el Artículo 83.5 del RGPD.

CUARTO: En fecha 17/02/21 se recibe escrito de alegaciones de la reclamada argumentado lo siguiente *“que las cámaras ya estaban instaladas previamente y que no están operativas, careciendo de monitor de visualización, permaneciendo en el inmueble al cumplir una función disuasoria”*.

“Debido a que no disponen de funcionamiento ni registran actividad alguna tampoco son un obstáculo para el ejercicio de la actividad, los arrendatarios no han realizado ningún acto ni solicitud autorización a los propietarios del inmueble para su desmantelamiento”.

“Es posible comprobar su inutilidad con la simple visita de la FFCC y que estas verifiquen lo que la compareciente alega y en su caso, cabría instar al propietario del inmueble su retirada”

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos

en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS

Primero. Los hechos traen causa de la reclamación de fecha 06/07/20 por medio de la cual se traslada la presencia de cámaras de video-vigilancia que presuntamente están orientadas hacia espacio público sin causa justificada.

Se adjunta Anexo Documental I con cinco fotografías que acreditan al presencia de los dispositivos objeto de denuncia.

Segundo. Consta identificado como principal responsable **A CULLER DE TERESA, S.L** quien no niega la presencia de las cámaras de video-vigilancia.

Tercero. Consta acreditada la presencia de tres cámaras en la fachada del inmueble con una palmaria orientación hacia zona pública, desprovistas de cartel informativo al respecto.

Cuarto. Según manifestación de la reclamada las cámaras no están operativas, cumpliendo una mera función disuasoria, de manera que estaban instaladas en el local, siendo fácilmente comprobable tal carácter.

Quinto. No consta acreditado ningún tratamiento de datos con las cámaras objeto de denuncia.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del Reglamento (UE) 2016/679, de 27 de abril, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), reconoce a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y resolver este procedimiento.

II

De acuerdo con la definición de “*datos personales*” que ofrece el artículo 4.1 del RGPD, la imagen de una persona física tiene el carácter de dato personal. Así pues, conforme al artículo 1.2 del RGPD, la imagen de una persona física ha de ser objeto de la protección dispensada por este Reglamento.

El RGPD dispone en su artículo 5, bajo la rúbrica “*Principios relativos al tratamiento*”:

“1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

La LOPDGDD dedica el artículo 22 a los “Tratamientos con fines de videovigilancia” y dispone:

“1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atentan contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes

deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2015/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.”

Entre los principios que presiden el tratamiento de los datos de carácter personal el artículo 5.1.c) del RGPD se refiere al de “*minimización de datos*”: “*Los datos personales serán: (...) c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*”.

Este principio está íntimamente conectado con la finalidad perseguida por el tratamiento de datos realizado. A su vez, conforme al artículo 22 de la LOPDGDD, el tratamiento que se efectúa mediante sistemas de videocámaras en supuestos como el que nos

ocupa debe tener la finalidad específica de *“preservar la seguridad de las personas y bienes, así como de sus instalaciones”*.

En consecuencia, el tratamiento de los datos personales con fines de videovigilancia deberá ser ajustado y proporcionado a la finalidad a la que se dirige y ser el estrictamente necesario para cumplir tal finalidad. Deberá restringirse el tratamiento de datos que exceda de tal finalidad o, proceder, en su caso, a su supresión.

En congruencia con el principio de minimización de datos la LOPDGDD advierte en su artículo 22.2 que *“Sólo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.”* Esto, porque el tratamiento de imágenes en lugares públicos puede ser realizado exclusivamente -previo el cumplimiento de los requisitos legalmente exigibles- por las Fuerzas y Cuerpos de Seguridad.

Para que la excepción mencionada en el artículo 22.2 de la LOPDGDD pueda aplicarse será necesario que no exista una ubicación alternativa de la videocámara desde la que no se capten imágenes de la vía pública. En tal caso, el responsable del tratamiento adecuará el uso de la instalación de modo que el impacto en los derechos de terceros (viandantes) sea el mínimo posible. No se admitirá el uso de prácticas de vigilancia más allá del entorno objeto de la instalación del sistema sin que pueda afectar a los espacios públicos circundantes como edificios contiguos y vehículos distintos de los que accedan al espacio vigilado. El principio de *“minimización de datos”* deberá respetarse tanto en el momento de la recogida de los datos como en el tratamiento posterior de ellos.

Cabe añadir, además, que el tratamiento de datos que se efectúa a través de sistemas de videovigilancia como el que es objeto de la presente reclamación, solo será lícito si se funda en la circunstancia legitimadora descrita en el artículo 6.1.e) del RGPD: *“el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”*. Precepto en el que nuevamente el RGPD exige que el tratamiento efectuado se limite a aquél que sea *necesario*, en este caso para cumplir una misión realizada en interés público. Esta misión, por aplicación del artículo 8.2. de la LOPDGDD en relación con el artículo 22 de la LOPDGDD, sólo puede ser, en supuestos como el que examinamos, la de preservar la seguridad de las personas y bienes.

III

El tratamiento de los datos personales está también presidido en el RGPD por el principio de *“transparencia”* (artículo 5.1.a). Este principio se hace efectivo a través de la obligación que el RGPD impone al responsable del tratamiento de informar al titular de los datos en los términos de los artículos 12, 13 y 14.

El artículo 12.1 del RGPD señala: *“1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14”*. El RGPD determina qué información debe de facilitarse al interesado respecto al tratamiento de sus datos personales y diferencia a tal efecto dos supuestos: que los datos se recaben del propio titular (artículo 13 RGPD) o que se obtengan de otra fuente (artículo 14 RGPD).

El artículo 13 del RGPD dispone:

“1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.”

Respecto al medio a través del cual el responsable del tratamiento puede ofrecer al afectado la información que preceptivamente debe de proporcionarle, el artículo 12.7 RGPD indica: “La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible, y claramente legible una adecuada visión de conjunto del tratamiento previsto”.

El artículo 22.4 de la LOPDGDD, transcrito en el Fundamento Jurídico precedente, con el propósito de que pueda cumplirse de una manera concisa y comprensible el deber de informar al interesado que el artículo 12 del RGPD impone al responsable del tratamiento, y al amparo de la previsión del artículo 12.7 del RGPD, articula un sistema de *información por capas*.

La primera capa -que ha de referirse, al menos, a la existencia del tratamiento; a la identidad del responsable y a la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD- se contendrá en un dispositivo cuyo diseño y ubicación deben ser tales que el afectado tenga una visión clara de la información disponible sobre el tratamiento de sus datos personales y sobre dónde y cómo encontrar la información detallada. No resultará necesario especificar la ubicación exacta del equipo de videovigilancia, pero, sin embargo, sí deberá quedar bien claro cuál es el ámbito o espacio sometido a videovigilancia.

La información de la segunda capa tiene que estar disponible en un lugar fácilmente accesible al afectado, ya sea una hoja informativa en una recepción, cajero, etc. ..., colocada en un espacio público visible o en una dirección web y habrá de referirse al resto de los aspectos que deben ser objeto de información con arreglo al artículo 13 del RGPD.

IV

A modo de resumen, tomando en consideración tanto lo expuesto en los Fundamentos precedentes como el conjunto de las disposiciones que regulan esta materia, para que

el tratamiento de la imagen de las personas físicas a través de sistemas de videovigilancia sea respetuoso con la normativa vigente de protección de datos personales deberá de cumplir estos requisitos:

- El tratamiento de datos debe de ser proporcionado en relación con la finalidad que legitima dicho tratamiento, *“preservar la seguridad de las personas y bienes, así como de sus instalaciones”*.

- Cuando el sistema esté conectado a una central de alarma, únicamente podrá ser instalado por una empresa de seguridad privada que cumpla los requisitos del artículo 5 de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

- Las videocámaras no podrán captar imágenes de las personas que se encuentren fuera del espacio privado en donde esté instalado el sistema de videovigilancia ya que el tratamiento de imágenes en lugares públicos sólo puede ser realizado, salvo que concurra autorización gubernativa, por las Fuerzas y Cuerpos de Seguridad. Tampoco pueden captarse ni grabarse espacios propiedad de terceros sin el consentimiento de sus titulares, o, en su caso, de las personas que en ellos se encuentren.

Esta regla admite alguna excepción ya que, en ocasiones, para la protección de espacios privados en los que se hayan instalado cámaras en fachadas o en el interior, puede ser necesario, para garantizar la finalidad de seguridad, la grabación de una porción de la vía pública.

Es decir, las cámaras y videocámaras instaladas con fines de seguridad no podrán obtener imágenes de la vía pública salvo que resulte imprescindible para dicho fin, o resulte imposible evitarlo por razón de la ubicación de aquéllas. Y, extraordinariamente, también se recogerá el espacio mínimo para dicha finalidad. Por lo tanto, las cámaras podrían excepcionalmente captar la porción de espacio público mínimamente necesaria para la finalidad de seguridad que se pretende.

- El deber de informar a los afectados previsto en los artículos 12 y 13 del RGPD y 22 de la LOPDGDD, en los términos ya señalados.

- El responsable del tratamiento deberá llevar un registro de actividades de los tratamientos efectuados bajo su responsabilidad en el que se incluya la información a la que hace referencia el artículo 30.1 del RGPD.

- Las cámaras instaladas no pueden obtener imágenes de espacio privativo de tercero y/o espacio público sin causa justificada debidamente acreditada ni pueden afectar a la intimidad de transeúntes que circulen libremente por la zona. No está permitida, por tanto, la colocación de cámaras hacia la propiedad privada de vecinos con la finalidad de intimidarlos o afectar a su ámbito privado sin causa justificada.

- En ningún caso se admitirá el uso de prácticas de vigilancia más allá del entorno que es objeto de la instalación, no pudiendo afectar a los espacios públicos circundantes, a edificios contiguos o a vehículos distintos de los que accedan al espacio vigilado.

Para facilitar la consulta la Agencia Española de Protección de Datos, a través de su página web [<https://www.aepd.es>], ofrece acceso a la legislación en materia de protección de datos personales, incluyendo el RGPD y la LOPDGDD (apartado *“Informes y resoluciones”* / *“normativa”*); a la Guía sobre el uso de videocámaras para seguridad y otras finalidades y a la Guía para el cumplimiento del deber de informar (ambas disponibles en el apartado *“Guías y herramientas”*).

También resulta de interés en el caso de que se realicen tratamientos de datos de bajo riesgo, la herramienta gratuita Facilita (en el apartado *“Guías y herramientas”*) que, mediante unas preguntas concretas, permite valorar la situación del responsable res-

pecto del tratamiento de datos personales que lleva a cabo y, en su caso, generar diversos documentos, cláusulas informativas y contractuales, así como un anexo con medidas de seguridad orientativas consideradas mínimas.

V

La reclamación que examinamos versa sobre dos cuestiones. Por una parte, plantea que la grabación de imágenes que se realiza por el sistema de videocámaras del reclamado excede de los límites permitidos pues capta la vía pública. Por otra, sobre la ausencia de cartel informativo de zona videovigilada que facilite la información que preceptivamente debe proporcionar el responsable del tratamiento.

La documentación que obra en el expediente confirma que existen tres videocámaras instaladas en distintas zonas del muro de un edificio donde, a tenor de lo manifestado por la reclamante, está ubicado el local de negocio del que es titular el reclamado.

El reclamado (a) en alegaciones de fecha 17/02/21 argumenta que las cámaras no están operativas, de manera que no realizan tratamiento de dato alguno, cumpliendo una mera función disuasoria.

Por tanto, no realizan un tratamiento de datos asociado a persona identificada o identificable, motivo por el que no puede hablarse de infracción en la materia que nos atañe.

La mera visualización exterior no es incompatible con la inoperatividad de las mismas, lo que ayuda a cumplir la labor disuasoria de estas en aras de la protección del inmueble y sus enseres.

Conviene recordar que la mala colocación de las cámaras aún siendo disuasorias no están exento de reproche en el marco de otras ramas del derecho, pudiendo ser considerada la conducta descrita como un ilícito civil, al desconocer los transeúntes de la zona el carácter simulado de las mismas, por lo que en aras de evitar males mayores es recomendable en estos casos una orientación hacia la zona privativa del local a proteger, evitando con ello un cierta intimidación con las cámaras a terceros que siente afectados por las mismas en la creencia de que están operativas.

La reciente Sentencia del TS Sala de lo Civil, sección 1ª, de 7 de noviembre de 2019, nº 600/2019, rec. 5187/2017, EDJ 2019/724119, razona que cuando un individuo desconoce que está siendo filmado se comporta con una naturalidad y espontaneidad que no se dan en caso contrario.

El TS trae a colación la doctrina del TC por la que *“la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad”*.

Aunque en el pasado la AEPD ha sancionado a responsables del tratamiento por el uso de este tipo de dispositivos, actualmente se entiende que el uso de cámaras simuladas no supone una infracción del derecho fundamental a la protección de datos.

La presencia de cámaras falsas orientada hacia espacio público puede generar nuevas reclamaciones en la creencia de la operatividad de las mismas, no teniendo los transeúntes que soportar la incertidumbre sobre si sus datos están siendo tratados o no, al margen que la medida es desproporcionada, pues bastaría una simple reorientación hacia los principales accesos y fachada del inmueble para que las mismas cumplieran igualmente su función.

Por los mismos motivos expuestos, no es necesario la señalización de zona video-vigilada al no realizarse en puridad un tratamiento de datos efectivos, si bien la ausencia de distintivo informativo, contribuye a aumentar la sensación de inseguridad en el vecindario al creerse objeto de grabación y desconocer el responsable y/o finalidad del tratamiento de las imágenes.

La presunción de inocencia rige sin excepciones en el Ordenamiento sancionador y ha de ser respetada en la imposición de cualquier sanción, ya sea penal o administrativa (TCO 13/1981), pues el ejercicio del derecho sancionador en cualquiera de sus manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

Conforme a este principio, no puede imponerse sanción alguna en razón de la culpabilidad del imputado si no existe una actividad probatoria de cargo, que en la apreciación de las autoridades u órganos llamados a resolver, destruya esta presunción (TCO Auto 3-12-81).

La cuestión del responsable en su caso de la retirada de las cámaras no compete a esta Agencia, pues son las partes (arrendador/arrendatario) las que deberán examinar la situación descrita, llegando a una solución que permita el equilibrio entre los intereses en conflicto, de tal manera que sea factible la protección del inmueble frente a supongamos actos vandálicos y la tutela de los derechos de los vecinos (as) que se sienten intimidados por el sistema denunciado.

VI

De acuerdo a lo expuesto procede ordenar el Archivo del presente procedimiento al no quedar acreditada la comisión de infracción administrativa alguna, al tener las cámaras un carácter **simulado** con fines de protección del local y sus enseres.

No obstante lo anterior, sin perjuicio de una comprobación in situ de las mismas por parte de este organismo, se recomienda la reorientación de estas, de manera que no estén orientadas hacia zona pública, sino hacia el espacio privativo necesario para cumplir su función de protección en los términos expuestos.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

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

PRIMERO: ORDENAR el **ARCHIVO** del presente procedimiento al no quedar acreditada al comisión de infracción administrativa alguna en la materia que nos ocupa.

SEGUNDO: NOTIFICAR la presente resolución a la entidad **A CULLER DE TERESA, S.L.**

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 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 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

938-131120

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