



Expediente N°: E/05084/2016

## RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **A.A.A. S.L.** en virtud de denuncia presentada por D<sup>a</sup>. **B.B.B.** y teniendo como base los siguientes

### HECHOS

**PRIMERO:** Con fecha 23 de agosto de 2016, tiene entrada en esta Agencia escrito de D<sup>a</sup>. **B.B.B.** (en adelante la denunciante), comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es la entidad **A.A.A. S.L.** (en adelante el denunciado), instaladas en la guardería infantil titularidad de dicha sociedad ubicada en **(C/...1) (VIZCAYA)**.

La denunciante manifiesta que la guardería dispone de un sistema de cámaras para que los padres puedan ver online a sus hijos durante hora y media y que se utilizan para control laboral.

Con fecha 5 de octubre de 2016, tiene entrada un nuevo escrito de la denunciante aportando fotografías de las cámaras denunciadas e impresión de pantalla de las páginas de Facebook, en las que la entidad se publicita, en las que informan de que disponen de un sistema de cámaras web y una intranet privada, que ofrece imágenes de las diferentes aulas durante la jornada escolar con Usuario y Contraseña para acceder de forma segura.

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

Con fecha 7 de marzo de 2017 se solicita información al responsable del establecimiento teniendo entrada en esta Agencia con fecha 21 de marzo de 2017 escrito del denunciado en el que manifiesta:

- El sistema de videovigilancia fue instalado por la empresa Alpex Digital SL. Aportan copia del contrato suscrito con dicho fin.
- La finalidad del sistema de videovigilancia es que los padres puedan ver a sus hijos en la guardería realizando las actividades diarias.
- Aportan fotografía del cartel informativo de la existencia de cámaras de videovigilancia. Dicho cartel se ubica en la entrada a la guardería y es visible antes del acceso a las instalaciones. El cartel contiene información del responsable ante el que se puede ejercer los derechos de protección de datos de carácter personal.
- Aportan un ejemplar del documento que suscriben los padres para dar el consentimiento para la recogida de las imágenes a través de cámaras. Dicho documento incluye entre otras las siguientes cláusulas:

*“Tanto el padre como la madre (en adelante conjuntamente como Los Padres) consienten como titulares de la patria potestad del niñ@ la cesión de los datos personales propios y del niñ@ a A.A.A. S.L., con CIF \*\*\*CIF. 1 (en adelante la Haurreskola A.A.A.) para que ios puedan tratar en el desarrollo de su objeto social. Así mismo, garantizan que han obtenido el consentimiento para la cesión y tratamiento de los datos de “otros autorizados”.*

*La persona abajo firmante, se responsabiliza de comunicar a la otra figura paterna y a cuantos tutores legales pudiera tener el bebo matriculado, de la incorporación a la guardería, eximiendo a Haurreskola A.A.A. de cualquier responsabilidad de comunicación.*

*La formalización de la presente matrícula por parte de los Padres, implica la aceptación expresa en su caso, de las condiciones generales de contratación y el consentimiento a la cesión y tratamiento de los datos de todas las personas relacionadas en la cláusula anterior. En particular, implica la aceptación, conocimiento y autorización, a que terceros (ej.: otros padres) puedan ver imágenes del niñ@ a través del servicio de supervisión y video vigilancia que ofrece la Haurreskola A.A.A. a todos los padres, al coincidir con otros niñ@s en la Haurreskola A.A.A..*

...”

- El sistema se compone de 4 cámaras ubicadas en las aulas y enfocadas hacia el aula, son fijas y no disponen de zoom.
- Aportan fotografía para acreditar la ubicación del monitor desde donde se visualizan las imágenes captadas por las cámaras. Dicho monitor se encuentra en un espacio cerrado con llave al que sólo tiene acceso el personal autorizado por la empresa.
- El acceso a las cámaras está permitido a la empresa Alpex Digital S.L. con la única finalidad del mantenimiento del sistema de vigilancia. Al sistema de videovigilancia solamente accede el personal autorizado. Aportan contrato de delegación del tratamiento de datos de carácter personal con la empresa Alpex Digital SL.
- El sistema de grabación se realiza mediante tarjetas SD con una conservación máxima de 15 días. Las personas autorizadas al acceso de dichas grabaciones son la Administradora de la empresa y socio capitalista.
- En cuanto al procedimiento empleado para informar a los trabajadores de la finalidad de la instalación de las cámaras, se les entrega un documento en el cual se le informa expresamente de la existencia de dichas cámaras, su finalidad y consienten expresamente dicho tratamiento firmando dicho documento. Adjuntan documento al respecto.
- Aportan copia del acuerdo de inscripción en el Registro General de Protección de Datos del fichero de videovigilancia con el código **\*\*\*COD.1**.

Con fecha 15 de junio de 2017 tiene entrada un nuevo escrito se **A.A.A. S.L.**, en el que, en respuesta al requerimiento de la inspección de datos sobre el consentimiento dado por D<sup>a</sup>. **B.B.B.** para el tratamiento de su imagen, manifiesta:

- Adjuntan el Documento que se le entregó a D<sup>a</sup>. **B.B.B.**, fechado el día 9 de marzo de 2016, en el que le informan de que sus datos van a ser incluidos en un fichero de la empresa y de sus derechos en relación al tratamiento de



datos de carácter personal.

- En la misma fecha manifiestan que se le informó verbalmente de la existencia del sistema de cámaras de seguridad y su finalidad.
- También manifiestan que el sistema de cámaras de seguridad es claramente identificado y visible. Aportan fotografía con la identificación del cartel de videovigilancia existente a la entrada de las instalaciones.
- Además, anteriormente a esa fecha, la trabajadora fue formada e informada por parte de la Franquicia, Franquicias A.A.A. SL, donde se le instruye en los procedimientos específicos de las Guarderías A.A.A., dentro de los cuales está la existencia de cámaras web en el centro de trabajo, de manera que así las familias pueden conectarse y ver a los hijos realizando las actividades diarias.

## **FUNDAMENTOS DE DERECHO**

### **I**

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

El artículo 126.1, apartado segundo, del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal establece:

*Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.*

### **II**

En primer lugar, procede situar el contexto normativo en materia de videovigilancia. Así el artículo 1 de la LOPD dispone: *“La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”*

En cuanto al ámbito de aplicación de la LOPD, el artículo 2.1 de la misma señala: *“La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”,* definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*.



El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”*.

El artículo 5.1. f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, define datos de carácter personal como: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”*.

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *“toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático”*. Sigue señalando: *“Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”*.

La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

Por su parte, la citada Instrucción 1/2006, dispone en su artículo 1.1 lo siguiente:

*“1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.”*

*El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales*



*relacionados con aquéllas.*

*Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.*

*Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.”*

La Instrucción 1/2006 en su artículo 2 establece lo siguiente:

*“1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

*2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.”*

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

De acuerdo con los preceptos transcritos, la cámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas que las hacen identificadas o identificables y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere.

### III

En el presente expediente se denuncia, por parte D<sup>a</sup>. **B.B.B.** la existencia de cámaras de videovigilancia, instaladas en la guardería infantil titularidad de dicha sociedad ubicada en **(C/...1) (VIZCAYA)**. La denunciante manifiesta que la guardería dispone de un sistema de cámaras para que los padres puedan ver online a sus hijos durante hora y media y también se utilizan para control laboral.

En el presente caso, se plantea por una lado el posible control laboral de los trabajadores con el sistema de videovigilancia instalado en el guardería y por otro, la visualización vía online de las imágenes de los menores en las aulas durante hora y media al día, por parte de los padres.

En la primera cuestión, se plantea si es necesario el consentimiento inequívoco de los trabajadores cuando se instalan cámaras de videovigilancia en el centro de trabajo,

al amparo del artículo 6.1 de la LOPD.

A este respecto es necesario realizar varias aclaraciones respecto al consentimiento en el ámbito laboral. Así, el consentimiento, elemento base en el tratamiento de los datos, entraña cierta complejidad, especialmente cuando nos referimos al ámbito laboral, dado que resulta de difícil cumplimiento que en ese ámbito concurren los requisitos legalmente previstos para considerar que se ha obtenido libremente el consentimiento. El artículo 3 h) de la LOPD lo define como *“Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que el conciernen”*.

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

b) Específico, es decir referido a un determinado tratamiento o serie de tratamientos concretos y en el ámbito de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

El apartado 2 del artículo 6 de la LOPD exige del necesario consentimiento cuando los datos se refieran *“a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento...”*

En el ámbito laboral, el Ordenamiento el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo de 24 de Octubre de 1995, los poderes de Dirección del empresario y es en éste articulado donde hallamos la oportuna legitimación.

El artículo 20.3 del Estatuto de los Trabajadores (ET) dispone que *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales,*



*guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso”.*

De todo ello se desprende que el empresario, en este caso la entidad denunciada, se halla legitimada para tratar las imágenes de los trabajadores en el ámbito laboral, al amparo del artículo 20.3 del ET. Ahora bien, esta legitimación no es absoluta y exige por parte del empresario la obligación de informar de dicho tratamiento a los trabajadores (cumpliendo así con el deber de informar previsto tanto en el artículo 10 de la Directiva 95/46/CE como en el artículo 5 de la LOPD.).

Es necesario en este punto diferenciar si la instalación de la cámara en el centro de trabajo es como medida de vigilancia y control del empresario, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales o si es una medida de seguridad para proteger la instalación y sus empleados.

En el primer caso, es decir cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, se aplicaría toda la normativa y jurisprudencia recogida “ut supra”, es decir sería necesario por parte del empresario, garantizar el derecho de información en la recogida de las imágenes, mediante información a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral.

En el segundo caso, es decir cuando la finalidad es de vigilancia y protección de las instalaciones y personal de la empresa, es necesario el cumplimiento de la LOPD, el Reglamento de Desarrollo de la LOPD y la Instrucción 1/2006. Por lo tanto, debería cumplirse, entre otros, el deber de información recogido en el artículo 5 de la LOPD, disponiendo de distintivos informativos de zona de videovigilancia acordes a la Instrucción 1/2006 e impresos informativos.

Así, el tratamiento de las imágenes por parte del responsable, obliga a que se cumpla con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD el cual reza lo siguiente:

*“1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

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

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

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

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

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

En cuanto al modo en que hay de facilitarse la información recogida en el artículo 5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que establece lo siguiente:

*“Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:*

*a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y*

*b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.*

*El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.”*

*“ANEXO-*

*1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.”*

En el caso que nos ocupa, la entidad denunciada, ha aportado fotografía de la existencia de cartel informativo de zona videovigilada, ubicado en la entrada a la guardería, claramente visible antes del acceso a las instalaciones. Dicho cartel es acorde al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD.

Por otro lado, en cuanto al procedimiento empleado para informar a los trabajadores de la finalidad de la instalación de las cámaras, se les entrega un documento en el cual se le informa expresamente de la existencia de dichas cámaras, con finalidad tanto de vigilancia interior de las instalaciones y para prevenir riesgos que afecten a la seguridad y protección de las personas, locales y bienes; como de control de calidad y rendimiento laboral de los trabajadores, verificando el cumplimiento del mismo de sus obligaciones y deberes laborales.

Así mismo aportan el Documento que se le entregó a la denunciante fechado el día 9 de marzo de 2016, en el que le informan de que sus datos van a ser incluidos en un fichero de la empresa y de sus derechos en relación al tratamiento de datos de carácter personal. Manifiestan que en la misma fecha se le informó verbalmente de la existencia del sistema de cámaras de seguridad y su finalidad.

Además, anteriormente a esa fecha, la trabajadora fue formada e informada por parte de la Franquicia, Franquicias A.A.A. SL, donde se le instruye en los procedimientos específicos de las Guarderías A.A.A., dentro de los cuales está la



existencia de cámaras web en el centro de trabajo, de manera que así las familias pueden conectarse y ver a los hijos realizando las actividades diarias.

Por lo tanto la entidad denunciada cumple con el deber de información recogido en el artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD, informando tanto a las personas que acceden al establecimiento como a sus trabajadores de la existencia y finalidad del sistema de videovigilancia instalado.

#### IV

Respecto al cumplimiento de la inscripción de ficheros, el artículo 26.1 de la LOPD, recoge lo siguiente:

*“1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos”*

El responsable del fichero es el titular del fichero que contiene datos de carácter personal. Sobre él van a recaer las obligaciones que establece la LOPD. . El responsable del fichero, antes de disponerse a someter datos personales a tratamiento, deberá cumplir con los requisitos de la normativa de protección de datos, teniendo en cuenta su naturaleza y la naturaleza de los datos que va a someter a tratamiento.

El apartado d) del artículo 3 de la LOPD define al responsable del fichero o tratamiento como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. El artículo 43 de la LOPD sujeta a su régimen sancionador precisamente al responsable del fichero o tratamiento.

El reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, complementa esta definición en el apartado q) del artículo 5, en el que señala lo siguiente:

*“q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.*

*Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados”.*

El responsable del fichero es, en suma, quien debe garantizar el derecho fundamental de protección de datos personales de todas las personas cuyos datos almacena. Por ello, va a estar obligado a llevar a cabo una serie de actuaciones dirigidas a la protección de los datos, a su integridad y a su seguridad.

El responsable debe notificar su fichero a la Agencia Española de Protección de Datos, que dispondrá inscribirlo en el Registro General de Protección de Datos. La notificación de inscripción del fichero facilitará que terceros puedan conocer que se está produciendo un tratamiento con una finalidad determinada y los afectados tendrán la



oportunidad de ejercitar sus derechos ante el responsable.

Además este es el criterio que se hace constar en la Instrucción 1/2006 , al señalar en su artículo 7 que *“1-La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.*

*Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.*

*2.-A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.”*

En el caso que nos ocupa, costa inscrito, entre otros, el fichero denominado “Videovigilancia” en el Registro General de la Agencia Española de Protección de Datos.

## V

En segundo lugar, se plantea la cuestión del acceso online de los padres, a las imágenes de sus hijos una hora y media al día.

Todo tratamiento de dato personal ha de estar legitimado en los términos del art. 6 LOPD y siendo la imagen un dato personal debe tener tal condición, requiriendo bien el consentimiento del afectado, o bien alguna de las causas del art. 6.2 LOPD.

Para tales efectos, también cabe la legitimación amparada en el interés legítimo del art. 7.f) de la Directiva 1995/46/CE, que establece:

*“Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: (...) f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del Art. 1 de la presente Directiva”.*

El principio de interés superior del menor consagrado se consagra en el art. 2 de la Ley Orgánica 1/1996 de protección jurídica del menor, el cual, teniendo en cuenta la nueva redacción introducida por la Ley Orgánica 8/2015, establece lo siguiente:

*“Todo menor tiene derecho a que su interés superior sea valorado y considerado como primordial en todas las acciones y decisiones que le conciernan, tanto en el ámbito público como privado. En la aplicación de la presente ley y demás normas que le afecten, así como en las medidas concernientes a los menores que adopten las instituciones, públicas o privadas, los Tribunales, o los órganos legislativos primará el interés superior de los mismos sobre cualquier otro interés legítimo que pudiera concurrir”.*



En virtud de lo anterior, no sólo existe un principio de interés superior del menor que debe presidir toda actuación relacionada con los menores de edad, sino que se consagra en la legislación que las medidas que adopten las instituciones, el interés superior del menor debe primar sobre cualquier otro interés.

El interés superior está representado en la mayor protección tanto física como psicológica de los menores a través de sistemas de vigilancia, que pueden ser complementarios de otros, ha de prevalecer permitiendo así la implantación de tales sistemas. Sin perjuicio de que pudieran existir otros mecanismos de control, se entiende que la instalación de cámaras puede servir al interés superior del menor contribuyendo a una mayor seguridad.

Ahora bien, dicho interés superior del menor no tiene por qué ser omnímodo, permitiendo la implantación de todo tipo de sistemas, sobre todo en la medida en que, de conformidad con el art. 2.5, se puedan establecer medidas que sean conciliables con otros derechos fundamentales, en este caso el derecho a la protección de datos personales. Y la ponderación en este caso, si bien cediendo a favor de la posibilidad de establecer sistemas de videovigilancia en los términos indicados, implica que tales sistemas estén dotados de unas especiales cautelas de forma que se minimicen los riesgos que pueden concurrir para la protección de datos.

Por lo tanto, deberán imponerse estrictas medidas en cuanto al acceso a las imágenes, tanto en el visionado inicial como en los posibles accesos a las grabaciones. En este sentido, deben implantarse medidas de seguridad que aseguren el destino de las imágenes como dato personal a los fines previstos. Las pantallas de visionado deberán estar en lugares donde sólo pueden acceder quienes estén autorizados para ver las imágenes. En definitiva, las imágenes nunca serán de acceso general para el personal del centro, debiendo asegurarse que son utilizadas para el cumplimiento de sus fines.

Aunque las imágenes "per se" no estén sujetos a los niveles de seguridad medio o alto regulados en el Título VIII RDLOPD en relación con el artículo 9 de la LOPD, la ponderación aconseja que, junto con las medidas de seguridad de nivel básico que deben implantarse, puedan existir controles algo más rigurosos, como podría ser el control de acceso físico a los lugares donde estén los equipos físicos que den soporte a los sistemas de información.

Deberán cumplirse, por supuesto, todas las obligaciones derivadas de la normativa de protección de datos: permitir el ejercicio de los derechos de los interesados, en particular el derecho de acceso que podrían solicitar los padres, en virtud del artículo 13.1 RDLOPD, en conexión con el artículo 15 de la LOPD; inscribir fichero, medidas de seguridad y elaboración de documento de seguridad. Y todo ello con el fin de preservar el interés superior del menor.

El consentimiento para el tratamiento de los datos de los menores se encuentra regulado en el artículo 13 RDLOPD citado y exige la autorización paterna, materna o del representante legal cuando se trate de menores de edad.

Aplicando las consideraciones recogidas anteriormente al presente caso, se aporta por la entidad denunciada un ejemplar del documento que suscriben los padres

para dar el consentimiento para la recogida de las imágenes a través de cámaras. Dicho documento incluye entre otras las siguientes cláusulas:

*"Tanto el padre como la madre (en adelante conjuntamente como Los Padres) consienten como titulares de la patria potestad del niñ@ la cesión de los datos personales propios y del niñ@ a A.A.A. S.L., con CIF \*\*\*CIF. 1 (en adelante la Haurreskola A.A.A.) para que los puedan tratar en el desarrollo de su objeto social. Así mismo, garantizan que han obtenido el consentimiento para la cesión y tratamiento de los datos de "otros autorizados".*

*La persona abajo firmante, se responsabiliza de comunicar a la otra figura paterna y a cuantos tutores legales pudiera tener el bebé matriculado, de la incorporación a la guardería, eximiendo a Haurreskola A.A.A. de cualquier responsabilidad de comunicación.*

*La formalización de la presente matrícula por parte de los Padres, implica la aceptación expresa en su caso, de las condiciones generales de contratación y el consentimiento a la cesión y tratamiento de los datos de todas las personas relacionadas en la cláusula anterior. En particular, implica la aceptación, conocimiento y autorización, a que terceros (ej.: otros padres) puedan ver imágenes del niñ@ a través del servicio de supervisión y video vigilancia que ofrece la Haurreskola A.A.A. a todos los padres, al coincidir con otros niñ@s en la Haurreskola A.A.A..(...)*

*Los padres podrán ejercitar sus derechos de acceso, rectificación, cancelación u oposición dirigiéndose a las oficinas de Haurreskola A.A.A. Sopela...*

*..."*

Asimismo en otro documento, aportado por la entidad denunciada, de autorización que deben firmar los padres, se recoge que cada familia tendrá un usuario y contraseña únicos e intransferibles estando éstas cifradas a través de la Web.

El sistema se compone de 4 cámaras ubicadas en las aulas y enfocadas hacia el aula, son fijas y no disponen de zoom.

Respecto a la ubicación del monitor, remiten fotografía para acreditar la ubicación del mismo en un espacio cerrado con llave al que sólo tiene acceso el personal autorizado.

El acceso a las cámaras está permitido a la empresa Alpex Digital S.L. con la única finalidad del mantenimiento del sistema de vigilancia, con el que tienen suscrito contrato de servicios y de delegación del tratamiento de datos de carácter personal.

Las personas autorizadas al acceso de las grabaciones son la Administradora de la empresa y socio capitalista.

A la vista de lo expuesto y de la documentación aportada, se procede al archivo del presente expediente de actuaciones previas, al no apreciarse vulneración a la normativa de protección de datos.

Por lo tanto, de acuerdo con lo señalado

**SE ACUERDA:**

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **A.A.A. S.L.** y **D<sup>a</sup>.B.B.B.**

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD,



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

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 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

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