Informe 0475/2014

La consulta plantea la conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD), y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RDLOPD) del sistema de grabación audiovisual que pretende implantar en las aulas y salas de comedor de un centro de educación infantil. Plantea la utilización del sistema fundamentalmente para el control laboral de sus empleados, incluyendo infracciones laborales y control del ejercicio de sus funciones.

Se somete por tanto a esta Agencia una doble cuestión. Por un lado el uso de un sistema de videovigilancia en las aulas y salas de comedor de un centro de educación infantil y, por otro lado, la finalidad del mismo de control laboral de los profesores y trabajadores del centro. Estudiaremos en primer lugar si el sistema de videovigilancia queda sometido a la normativa de protección de datos, delimitando si una de las finalidades puede ser de control laboral de los trabajadores y las obligaciones que ello supondría para después examinar si cabe la implantación del sistema del modo propuesto por la consultante y, de ser positiva la respuesta, si cabe también el tratamiento de las imágenes de los menores.

I

Según la consultante, la finalidad del sistema de videovigilancia que pretende implantarse es eminentemente de control laboral. Por ello, comenzaremos estudiando dicha cuestión.

De conformidad con los artículos 1 y 2.1 LOPD, la normativa que nos ocupa tiene por objeto la protección de los datos de carácter personal como derecho fundamental, 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"*. La imagen de una persona es un dato personal, considerando también el artículo 5.1. f) RDLOPD, que como tales *"Cualquier información numérica, alfabética, gráfica,*

fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables". Y en este mismo sentido el Considerando 14 de la Directiva 95/46/CE que señala *"(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;"*.

Por su parte, 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"*. De acuerdo con esta definición de tratamiento de datos personales, la captación y en su caso grabación de imágenes de las personas constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada.

En este mismo sentido se pronuncia la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

Todo tratamiento de datos personales ha de estar legitimado por alguna de las causas del art. 6 LOPD. Pues bien, la captación y grabación de las imágenes de los empleados del centro con un fin de control laboral aparece amparado por el art. 6 LOPD, al existir una habilitación legal para el control laboral pretendido que es de carácter imperativo para "*las partes de un contrato… de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*".

El artículo 20.3 del Texto Refundido del Estatuto de los Trabajadores (ET), aprobado por Real Decreto Legislativo 2/2015 de 23 de octubre – cuyo tenor literal apenas ha cambiado respecto de la versión anterior en lo que ahora interesa - , 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 y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".

En este sentido, el artículo 20.3 ET en relación con el art. 6 LOPD legitimaría, en principio, a la consultante como empleadora para tratar las imágenes de los trabajadores en el ámbito laboral con carácter general.

Y así lo ha venido reiterando la jurisprudencia en lo que a empleados públicos se refiere amparado en el art. 6.2 LOPD, como en Sentencia de la Sala Tercera del Tribunal Supremo de 2 de julio de 2007 (Rec. 5017/2003) que señala que el control del cumplimiento del horario de trabajo a que vienen obligados los empleados públicos es inherente a la relación que une a estos con la Administración en cuestión, y no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Asimismo, la Sentencia de la misma Sala de 2 de julio de 2007 (Rec. 5017/2003) indica: *"Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos".*

Ahora bien, esta legitimación no es absoluta y exige que el empresario informe 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.). Y no sólo a los trabajadores, sino también a sus representantes. En este punto resulta ilustrativa y capital la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero, recurso de amparo 10522/2009, cuya conclusión es: *"Por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa (…) No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser*

dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo".

En este sentido hay que tener en cuenta la Sentencia de la Sala de lo Social del Tribunal Supremo de 13 de mayo de 2014, rec. 1685/2013 en un supuesto de despido de una trabajadora derivado de incumplimientos a través de las imágenes captadas por un sistema de videovigilancia, que dispone lo siguiente: *"por la empresa no se dio información previa a la trabajadora de la posibilidad de tal tipo de grabación ni de la finalidad de dichas cámaras instaladas permanentemente, ni, lo que resultaría más trascendente, tampoco se informó, con carácter previo ni posterior a la instalación, a la representación de los trabajadores de las características y alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, ni explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo"*

Y así ha venido aplicándose por esta Agencia, como en la Resolución recaída en el PS/00724/2014. En definitiva, el tratamiento de imágenes de los trabajadores con fines de control laboral está admitido con carácter general, al aparecer legitimado por el art. 20.3 ET, en la medida en que cumpla todos los requisitos de la LOPD incluyendo en todo caso la previa información a los trabajadores y a sus representantes.

II

Sin embargo, ello no implica que en el ámbito laboral quepa todo tratamiento de datos personales para el control por el empresario del cumplimiento de los deberes laborales del trabajador. Es decir, una cosa es la finalidad del tratamiento, que en este caso sería la prevista en el art. 20.3 ET, y otra la necesaria aplicación del principio de proporcionalidad consagrado en el art. 4.1 LOPD únicamente permitiendo el tratamiento de datos "*adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido*".

Respecto de la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de "*una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.*

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

Por consiguiente, cualquier medida de control que se adopte debe superar este juicio de proporcionalidad, determinando si la medida es adecuada, necesaria y equilibrada, ya que en otro caso resulta desproporcionada y por ello contraria a la normativa de protección de datos.

En definitiva, el control laboral como causa legitimadora para el tratamiento de datos personales no implica, *per se*, que quepa todo tratamiento de datos amparado en dicha finalidad. Y en el aspecto que nos ocupa relativo a la videovigilancia, el tratamiento de todas las imágenes que ocupan la jornada laboral de un trabajador, como mecanismo de seguimiento continuo y permanente de su actividad pudiera resultar excesivo al suponer una verdadera monitorización de los trabajadores, y sin que se ofrezca una causa concreta, temporalmente limitada y ponderada, como podría suceder si existiera un problema concreto con un trabajador determinado relativo al cumplimiento de sus deberes laborales. Se trata de una cuestión ampliamente abordada en diversos documentos internacionales que pasamos a estudiar.

Y es que en el ámbito estrictamente laboral, existen diversos documentos internacionales que abordan la problemática de la protección de datos en dicho ámbito. En el **Grupo de Berlín**, constituido en el seno de la Conferencia Internacional sobre Protección de Datos, el documento **"Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales" (agosto de 1996),** ya analiza los riesgos inherentes al control y vigilancia de los empleados a través de las Tecnologías de la Información y de las Comunicaciones, que suponen en muchas ocasiones una intrusión en su privacidad.

En dicho documento se estudian en primer lugar los métodos de recogida de datos más comunes utilizados en el seno de las organizaciones empresariales, tales como los dispositivos magnetofónicos, audio-visuales, transmisores de infrarrojos, identificadores de datos biométricos, dispositivos de videovigilancia, y comunicaciones electrónicas, alertando sobre los riesgos y perjuicios que el uso desviado de dichos medios puede ocasionar al trabajador. Y es que, en lo que ahora interesa, hace especial referencia a los sistemas de videovigilancia, en su caso utilizados en un primer momento con fines de seguridad privada, que graban datos personales de los trabajadores como hábitos de trabajo, relaciones conductuales con los compañeros de trabajo y con terceros no trabajadores en la empresa.

A modo de recomendación, y en orden a garantizar que tal uso será legítimo, necesario, adecuado, pertinente, y proporcionado a la finalidad que lo justifica, se establecen los necesarios controles, en los que se implica muy especialmente a los "representantes de los trabajadores". Así, tanto los trabajadores como sus representantes, deberán ser informados del tipo de tecnología utilizada por el empresario en relación con la vigilancia y seguimiento de su actividad laboral, debiendo abstenerse el empleador de recoger datos personales que resulten excesivos en razón de la propia naturaleza de la relación laboral. A su vez, los representantes de los trabajadores obtendrán cumplida información sobre la introducción de cualquier nuevo sistema de registro de datos que afecte al conjunto de los trabajadores, teniendo estos últimos la posibilidad de acceder a los datos que se procesen sobre ellos y el derecho a rectificar los posibles errores que les afecten.

Señala también, que salvo excepciones extremas, fundamentadas en una firme sospecha sobre la existencia de actividades delictivas o dolosas del trabajador, el derecho de Información en la recogida de datos constituye un

requisito indispensable para utilizar, en su caso, la información recabada en el lugar de trabajo contra el propio trabajador. En este supuesto, el empleado deberá tener la oportunidad de acceder a la información que le es adversa a fin de poder rebatirla.

Ahora bien, indica el documento en cuestión que las nuevas tecnologías de la información permiten la monitorización continua y la vigilancia en el lugar de trabajo. En determinados casos, la información sobre la actuación o el comportamiento personal de los trabajadores puede ser recopilada y utilizada secretamente para propósitos sobre los que los trabajadores no son conscientes.

Y en este sentido, uno de los parámetros a tomar en cuenta para determinar la proporcionalidad en el tratamiento de los datos son las expectativas razonables y legítimas de privacidad de los trabajadores, que deberán ser analizadas según las circunstancias del caso, sin que en ningún caso el tratamiento pueda ser contrario a su dignidad. Específicamente el informe estudiado afirma que si bien las razones de seguridad permiten que las máquinas sean vigiladas, puede ser excesivo extender la vigilancia a las personas que trabajan con tales máquinas.

Y en este punto es esencial que en ningún caso el empresario pueda tratar datos personales que no sean directamente relevantes en el ámbito de la relación laboral, como el comportamiento o las características personales de los trabajadores o los contactos internos con otros trabajadores o externos del trabajador. Este punto se torna en esencial, puesto que el sistema propuesto supondría la monitorización completa de los trabajadores, de modo que los sistemas de tratamiento de datos permitirían la supervisión de toda su actuación, tanto con los niños del centro de educación infantil como con otros trabajadores, permitiendo un constante seguimiento de su actuación, y excediendo por tanto notoriamente el poder directivo del empresario.

Por su parte, el **Grupo de Trabajo del artículo 29**, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE 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, en su **Dictamen 8/2001 (WP 48)**, sobre el tratamiento de datos personales en el contexto laboral, parte de la base de que muchas de las actividades realizadas de forma rutinaria en el

ámbito de la empresa implican el tratamiento de datos personales de los trabajadores y, en muchas ocasiones, de información de carácter personal especialmente protegida.

Indica el Dictamen 8/2001 que "*La recopilación, almacenamiento y uso de información sobre los trabajadores por medios electrónicos, y las diversas herramientas de uso común en buena parte de las empresas, tales como el correo electrónico o el acceso a Internet, implican en muchas ocasiones el tratamiento de datos personales de los trabajadores. A ello se unen otras nuevas modalidades de control del trabajador, que llegan de la mano de la imagen y el sonido, entre las que destacan los sistemas de videovigilancia a los que se debe aplicar la normativa sobre protección de datos*."

En el citado Dictamen, el Grupo enumera y desarrolla los Principios Fundamentales de la Protección de Datos, que los empresarios deberán tener siempre en cuenta en el contexto laboral. Así, los principios de Finalidad y de Transparencia, referidos a la necesidad del uso legítimo de los datos, adecuados a un fin determinado y explícito, propio de la actividad laboral, y a la necesidad de que los trabajadores conozcan qué datos recoge el empresario sobre ellos. Según se apunta en el Dictamen, la Transparencia también podría garantizarse otorgando al interesado el derecho de acceso a los datos personales que les afectan. De este modo, los trabajadores, como partes interesadas en la relación laboral, deben beneficiarse de los derechos que confiere la Directiva sobre protección de datos y, muy especialmente, del derecho de acceso, previsto en el artículo 12 de la misma.

El principio de legitimidad se vincula al de proporcionalidad, debiendo ser los datos recabados, adecuados, pertinentes y no excesivos en relación con la necesidad de su recogida, y disponiéndose la necesidad de que los trabajadores sean suficientemente informados sobre la existencia de dicho tratamiento legítimo y proporcionado. Así, en lo referente a la vigilancia de los trabajadores a través del correo electrónico, Internet, cámaras de vídeo o datos de localización, el control deberá ser una respuesta proporcionada del empresario ante riesgos potenciales, teniendo en cuenta el derecho a la vida privada y otros intereses de los trabajadores.

Y en lo que ahora interesa el dictamen contiene un apartado específicamente destinado a vigilancia y monitorización (apartado 12), mencionando específicamente el uso de videovigilancia. Afirma el texto que (la

traducción es nuestra) "*cualquier monitorización debe ser una respuesta proporcionada de un empresario a los riesgos a los que se enfrente, considerando la legítima privacidad y otros intereses de los trabajadores. Cualquier dato personal conservado o utilizado en el seno de una monitorización ha de ser adecuado, pertinente y no excesivo para la finalidad perseguida. Cualquier monitorización ha de ser llevada a cabo del modo menos intrusivo posible*". Y se enfatiza siempre en la necesidad de establecimiento de una medida proporcionada y lo menos intrusiva posible en la privacidad de los trabajadores.

De nuevo, este documento da respuesta a la cuestión estudiada, por cuanto el sistema planteado prevé, sin distinción, una monitorización de toda la actividad de los trabajadores. Otra cosa sería que se hubiera planteado el uso del sistema ante una situación concreta y particular de importantes incumplimientos concretos de deberes laborales, o únicamente durante pequeños periodos de tiempo o por motivos determinados que hicieran proporcional el uso del sistema. Ahora bien, la implantación de un sistema de videovigilancia de monitorización permanente de los trabajadores, además de ser excesivo por poder conseguirse las finalidades a través de mecanismos menos intrusivos, supondría un control que excedería del poder directivo, permitiendo el control de todos y cada uno de los comportamientos de los trabajadores, sin mencionar ningún riesgo potencial en particular, y suponiendo una importantísima intervención en la vida privada de los trabajadores. Una cosa es la tolerancia por los trabajadores de un determinado grado de intrusión en su privacidad, como parte de una organización empresarial, y otra distinta el uso ilimitado de estos mecanismos que podría atentar contra la dignidad de los trabajadores.

Si bien entendemos que la cuestión de la monitorización y la vigilancia permanente de los trabajadores ha quedado suficientemente estudiada, también puede mencionarse el **Documento de Trabajo del Grupo del Artículo 29, relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo de 29 de mayo de 2002 (WP 55),** en el que se examina la vigilancia por el empleador de la utilización del correo electrónico e Internet por parte de los trabajadores, ofreciendo una orientación y ejemplos concretos sobre lo que constituyen actividades de control legítimas y límites aceptables de la vigilancia de los trabajadores por el empresario.

Cabe destacar que dicho Documento de Trabajo señala respecto del principio de proporcionalidad que *"Según este principio, los datos personales, incluidos los que se utilicen en las actividades de control, deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben. La política de la empresa en este ámbito deberá adaptarse al tipo y grado de riesgo al que se enfrente dicha empresa.*

El principio de proporcionalidad excluye por lo tanto el control general de los mensajes electrónicos y de la utilización de Internet de todo el personal, salvo si resulta necesario para garantizar la seguridad del sistema. Si existe una solución que implique una intromisión menor en la vida privada de los trabajadores y que permita lograr el objetivo perseguido, el empleador debería considerar su aplicación (por ejemplo, debería evitar los sistemas que efectúan una vigilancia automática y continua)."

Más recientemente la **Recomendación CM/Rec (2015) 5 del Comité de Ministros del Consejo de Europa de 1 de abril de 2015 sobre el tratamiento de datos en el ámbito laboral**, partiendo la necesaria minimización de los riesgos para la privacidad de los empleados considerando los actuales métodos de tratamiento de datos derivados del uso de nuevas tecnologías, establece una serie de principios aplicables, según su artículo 1, al tratamiento de datos personales de los empleados en los sectores público y privado. En concreto, el artículo 15 contempla los sistemas de información y tecnologías para la monitorización de empleados, incluyendo videovigilancia. Y se recomienda que no se permitan estos sistemas y tecnologías cuando su finalidad "*directa y principal sea la monitorización de la actividad y comportamiento de los empleados*" (la traducción es nuestra). Únicamente se contempla su posible utilización, y siempre con las debidas salvaguardas, incluida la previa consulta de los representantes de los trabajadores, cuando sean empleados con otra finalidad y su consecuencia indirecta sea la posibilidad de tal monitorización. Asimismo se prevé en el apartado 15.2 que en tales supuestos los sistemas y tecnologías sean "específicamente diseñados y situados de forma que no socaven sus derechos fundamentales. El uso de videovigilancia para la monitorización de ubicaciones que son parte del área más personal de la vida de los empleados no está permitido en ninguna situación".

En definitiva, en ningún caso la instalación de un sistema de videovigilancia que permita un seguimiento continuo de la actividad de los

trabajadores de un centro de educación infantil monitorizando por completo su actividad laboral puede entenderse ajustado al principio de proporcionalidad debido a la intromisión en la vida privada que ello representa, al carácter amplio e ilimitado del sistema y a la posible utilización de otros medios alternativos que permitieran la consecución de los fines perseguidos según la consulta. En lo que atañe a la vida privada no podemos dejar de mencionar la **Sentencia del Tribunal Europeo de Derechos Humanos de 23 de noviembre de 1992, caso Niemitz contra Alemania**, en la que se indicó (apartado 29): "*El Tribunal no considera ni posible ni necesario buscar la definición exhaustiva de la noción de "vida privada". No obstante, sería demasiado restrictivo limitarla a un "círculo íntimo" donde cada uno puede llevar su vida personal como quiera, y separarla totalmente del mundo exterior a este círculo. El respeto a la vida privada debe incluir también, en cierta medida, el derecho de los individuos para establecer y desarrollar relaciones con sus semejantes.*

Parece, además, que no existe ninguna razón de principio para considerar esta forma de entender el concepto de "vida privada" como excluyendo las actividades comerciales o profesionales: después de todo, es en su trabajo donde la mayoría de las personas tiene muchas, incluso la mayoría de oportunidades para fortalecer sus vínculos con el mundo exterior. Un hecho señalado por la Comisión, lo confirma: en la actividad profesional de alguien, no siempre se puede desentrañar lo que entra dentro del ámbito profesional de lo que no. En especial, las tareas de un miembro de una profesión liberal pueden constituir un elemento de su vida en grado tan alto, que no podía decir en qué condición se encuentra en un momento dado".

Y también en este sentido la **Sentencia del mismo tribunal, Sección 3ª de 24 junio 2004 Asunto Von Hannover contra Alemania** señala: "*Además, la esfera de la vida privada, tal como la concibe el Tribunal, cubre la integridad física y moral de una persona; la garantía que ofrece el artículo 8 del Convenio está destinada principalmente a asegurar el desarrollo, sin injerencias externas, de la personalidad de cada individuo en la relación con sus semejantes (…)*

El Tribunal ha señalado igualmente que, en ciertas circunstancias, una persona dispone de una «esperanza legítima» de protección y de respeto de su vida privada".

Por tanto, en el asunto planteado en el presente informe es irrelevante que junto con las imágenes de los trabajadores el sistema propuesto implicara también el tratamiento de las imágenes de los menores, careciendo de sentido

que por esta Agencia se estudie si existe o no legitimación para el tratamiento de datos de los menores, por cuanto se ha apreciado que no cabe la utilización del sistema de videovigilancia para el control laboral de los trabajadores del centro de educación infantil en los términos expuestos.

III

Ahora bien, la consulta también se refiere, aunque tangencialmente, a la posible prevención de daños de los menores de edad, mencionando tanto "*el maltrato físico, verbal o psicológico*". En este sentido, y partiendo de la base que no puede implantarse un sistema de videovigilancia de los empleados del centro educativo con fines de control laboral de los mismos que suponga su monitorización, nos planteamos si cabe la implantación de tales sistemas, siempre en zonas comunes como el comedor o el patio, y no en las aulas, con fines de protección de los menores.

Procede, por tanto, estudiar si cabe el tratamiento de las imágenes de los menores en un ámbito escolar con un fin de protección de tales menores, ajeno por tanto al de control laboral planteado. Debemos cuestionarnos, si existe legitimación para el tratamiento de los datos de los menores, en este caso la captación y grabación del dato de la imagen.

Como es sabido, todo tratamiento de dato personal ha de estar legitimado en los términos del art. 6 LOPD. En el apartado anterior del presente informe ya hemos indicado que la imagen es un dato personal y que todo tratamiento ha de estar legitimado, requiriendo bien el consentimiento del afectado, bien alguna de las causas del art. 6.2 LOPD. Ahora bien, también cabe 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 Tribunal Supremo, en el recurso 25/2008 de la Sección 6ª de la Sala Tercera dirigido frente a determinados preceptos del RD 1720/2007, de 21 de diciembre, se cuestionó la adecuación o no al derecho comunitario del artículo

10.2.b) del RD 1720/2007, de 21 de diciembre, por lo que planteó una cuestión prejudicial al TJCE. Dicha cuestión prejudicial fue resuelta por el Tribunal de Justicia de las Comunidades Europeas, en Sentencia de 24 de noviembre de 2011, que contiene los siguientes pronunciamientos: "1*. Se opone al artículo 7.f) de la Directiva 95/46 la normativa nacional que, para permitir el tratamiento de datos, sin consentimiento, y necesario para la satisfacción de un interés legítimo (del responsable o del cesionario) exige que se respeten los derechos y libertades del interesado, y además que dichos datos figuren en fuentes accesibles al público, excluyendo de forma categórica y generalizada todo tratamiento que no figure en dichas fuentes.*
2. El artículo 7.f) de la Directiva 95/46 tiene efecto directo".

Este pronunciamiento del Tribunal de Justicia se sustenta, entre otras, en las siguientes consideraciones:
"*El artículo 7, letra f) establece dos requisitos acumulativos para legitimar el tratamiento de datos:*
Necesario para satisfacer un interés legítimo.
Que no prevalezcan derechos y libertades fundamentales del interesado. (Que requieran protección con arreglo al apartado 1 del Art. 1 de la presente Directiva).
El segundo requisito exige una ponderación de los derechos e intereses en conflicto que dependerá de las circunstancias concretas, teniendo en cuenta los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.
A efectos de tal ponderación la lesión de los derechos fundamentales del afectado por el tratamiento puede variar en función de que los datos figuren ya, o no, en fuentes accesibles al público.
Los tratamientos que figuren en fuentes no accesibles al público implican necesariamente que el responsable o el cesionario del tratamiento dispondrán en lo sucesivo de cierta información sobre la vida privada del interesado. Lesión, más grave, de los derechos del interesado consagrados en los artículos 7 y 8 de la Carta que debe ser apreciada en su justo valor, contrarrestándola con el interés legítimo del responsable o tercero.

Así pues, el artículo 7.f) de la Directiva 95/46/CE tiene efecto directo, siendo el interés legítimo presupuesto legitimador para el tratamiento de datos personales sin consentimiento del interesado, "siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección".

En este sentido, la Sección 1ª de la Sala de lo Contencioso Administrativo de la Audiencia Nacional viene realizando una ponderación caso por caso de la relación entre el interés legítimo y los derechos y libertades fundamentales del interesado. Así, la primera resolución que trató la cuestión fue la de 15 de marzo de 2012 dictada en el recurso 390/2010; respecto de la ponderación señalaba que "*Ponderación de intereses en conflicto que dependerá de las circunstancias concretas de cada caso y en la que no obstante, sí puede tomarse en consideración, a efectos de determinar la posible lesión de los derechos fundamentales del afectado, el hecho de que los datos figuren ya, o no, en fuentes accesibles al público. Más ello, simplemente, como un elemento más de ponderación*".

En el supuesto planteado, el interés legítimo no podría venir determinado, como resulta del apartado anterior de este informe, del propósito de la propia consultante, "*para que la empresa pueda verificar el cumplimiento por éstos [empleados en su actividad profesional] de sus obligaciones y deberes laborales*". Es decir, no cabe aplicar como principio legitimador el art. 58 del Texto Refundido del Estatuto de los Trabajadores en relación con el deber de los trabajadores de "*cumplir las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de buena fe y diligencia*" (art. 5.a) del mismo cuerpo legal.

A juicio de esta Agencia, el interés legítimo en este caso sólo podría plantearse en relación con el principio de interés superior del menor consagrado en el art. 2 de la Ley Orgánica 1/1996 de protección jurídica del menor, teniendo en cuenta la nueva redacción introducida por la Ley Orgánica 8/2015 en los siguientes términos: "*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 esta nueva redacción, 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 (institución que en el caso de la consulta es privada) el interés superior del menor debe primar sobre cualquier otro interés. Y decimos que el

interés superior del menor concurre en el caso planteado porque la propia consultante indica que existen circunstancias que conllevan que se adopten mecanismos para asegurar el bienestar físico y emocional de los niños; mecanismos que incluyen unos elementos de control no utilizados hasta ahora, como son los sistemas de videovigilancia. Se alude así a *"la corta edad de los niños… y su fragilidad física, psicológica y emocional, no podemos contrastar otra versión, en caso de accidentes*". Sin perjuicio que pudieran existir otros mecanismos de control, como son el control presencial realizado por el director o por otro personal del centro, entendemos que el incremento de los controles en cuestión pudiera servir al interés superior del menor contribuyendo a una mayor seguridad en los patios y en el comedor.

Así, la nueva redacción a que antes aludíamos del art. 2 de la Ley Orgánica de Protección Jurídica del Menor introduce en su apartado 2 una serie de criterios generales para interpretar y aplicar en cada caso el interés superior del menor, sin perjuicio de los establecidos en la legislación específica aplicable o de aquellos otros que puedan estimarse adecuados. Y en el apartado a) se refiere al "*desarrollo del menor y la satisfacción de sus necesidades básicas, tanto materiales, físicas y educativas como emocionales y afectivas*". Además, sitúa el interés superior del menor como prioritario, si bien aplicándose respetando los restantes intereses legítimos indicando el art. 2.5: "*En caso de concurrir cualquier otro interés legítimo junto al interés superior del menor deberán priorizarse las medidas que, respondiendo a este interés, respeten también los otros intereses legítimos presentes. En caso de que no puedan respetarse todos los intereses legítimos concurrentes, deberá primar el interés superior del menor sobre cualquier otro interés legítimo que pudiera concurrir. Las decisiones y medidas adoptadas en interés superior del menor deberán valorar en todo caso los derechos fundamentales de otras personas que pudieran verse afectados*".

Y es precisamente lo que procede realizar en el supuesto planteado, debiendo ponderarse, por un lado, el interés superior del menor en conexión con el interés del centro escolar en realizar debidamente sus funciones para con los menores; y por otro lado el derecho a la protección de datos personales de los menores, al captar y grabar sus imágenes los sistemas de videovigilancia propuestos. En este sentido, partimos de la base de que el interés superior del menor implica que los centros docentes estén obligados a cuidar a los menores debidamente y prevenir la comisión de ilícitos, no sólo penales sino también civiles, para con ellos. Así se plasma en la legislación

sobre educación, como la garantía de calidad de los centros educativos de los artículos 14 de Ley Orgánica 8/1985, de 3 de julio y 67.2 de la Ley Orgánica 10/2002, de 23 de diciembre de calidad de la educación, así como la regulación del Título IV de la Ley Orgánica 1/1990, de 3 de octubre relativa a la calidad de la enseñanza en la parte no derogada y en los criterios introducidos por Ley Orgánica 8/2013, de 9 de diciembre de mejora de la calidad educativa. Todo ello puesto en relación con el Código Civil, que entre las obligaciones extracontractuales que nacen de la culpa o negligencia prevé en el art. 1903 la de "*las personas o entidades que sean titulares de un Centro docente de enseñanza no superior* [que] *responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del Centro, desarrollando actividades escolares o extraescolares y complementarias*".

La solución parece aparentemente resuelta en el art. 2.5 de la Ley Orgánica 1/1996 transcrito. El interés superior del menor, en este punto manifestado en la mayor protección tanto física como psicológica de los menores a través de nuevos sistemas de vigilancia, que pueden ser complementarios de otros, ha de prevalecer permitiendo así la implantación de tales sistemas. 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.

Así, en primer lugar, los sistemas permitirán únicamente la captación y reproducción de las imágenes estrictamente necesarias para el cumplimiento de los fines propuestos. Se plantea así su uso en el patio y en el comedor, no en lugares como las aulas en las que con fines de control laboral implicaría una monitorización permanente de los empleados en los términos ya estudiados; además también habrá de tenerse en cuenta este criterio en la orientación de las cámaras. Por supuesto en ningún caso podrán captar la vía pública, de conformidad con la Ley Orgánica 4/1997, pero es que tampoco podrán captar lugares donde no se encuentren menores por no servir a la finalidad prevista.

En segundo lugar, deberán imponerse estrictas medidas en cuanto al acceso a las imágenes, tanto en el visionado inicial como en los posibles accesos a las grabaciones. Las pantallas de visionado no podrán estar en lugares de acceso general, sino en lugares donde sólo puedan acceder quienes puedan ver las imágenes. Y únicamente se permitirá tanto su visionado inicial como el acceso ulterior a las imágenes grabadas al director del centro, o a la persona responsable que tenga a su cargo la gestión de los recursos humanos, o la persona específicamente designada por el centro para realizar un seguimiento del cumplimiento de los deberes del centro en relación con la garantía de la integridad física y moral de los menores. En definitiva, las imágenes nunca serán de acceso general para el personal del centro, debiendo asegurarse que sólo son utilizadas para el cumplimiento de los fines anteriormente indicados.

En este sentido, deberían implantarse medidas de seguridad que aseguraran el destino de las imágenes como dato personal a los fines previstos. Aunque las imágenes *per se* no estén sujetas a los niveles de seguridad medio o alto regulados en el Título VIII RDLOPD en relación con el art. 9 LOPD, la ponderación que estamos realizando aconseja que, junto con las medidas de seguridad de nivel básico que deban implantarse, puedan existir controles algo más rigurosos, como podría ser el control de acceso físico a los lugares donde estén instalados los equipos físicos que den soporte a los sistemas de información o la implantación de un registro de accesos. Estas medidas, u otras similares que impliquen una mayor protección de las imágenes, podrían contribuir a asegurar la ponderación entre los principios estudiados.

También contribuiría a la ponderación que estamos realizando la implantación de unos periodos de conservación muy reducidos para la conservación de las imágenes guardadas. La Instrucción 1/2006 establece en su artículo 6 un plazo de un mes desde su captación. Pero podría incluso reducirse ese plazo, teniendo en cuenta que si hubiera acaecido un suceso que afectara a los menores debería ser apreciado en un lapso de tiempo mucho más breve. Así, entendemos que podría establecerse un plazo de diez días, que por un lado es inferior a un mes pero suficientemente extenso para que el centro docente haya podido percatarse de la existencia de un perjuicio concreto y específico para el menor que pudiera tener consecuencias jurídicas, coincidiendo así con el plazo para el ejercicio del derecho de cancelación de los datos, y conciliado con la protección de los datos personales. Transcurrido

dicho plazo de diez días sólo podrían conservarse las imágenes que revelaran algún tipo de hecho trascendente en relación con el interés superior del menor.

Y deberán cumplirse, por supuesto, todas obligaciones derivadas de la normativa de protección de datos. Por un lado, permitirse el ejercicio de los derechos de los interesados, en particular el derecho de acceso que podrían solicitar los padres en virtud del art. 13.1 RDLOPD en conexión con el art. 15 LOPD. También deberán inscribirse los ficheros en el Registro General de Protección de Datos y cumplirse las restantes medidas de seguridad, como la elaboración de un documento de seguridad. Y en todo caso preservarse la finalidad alegada para el uso de los datos, que no es otra que el interés superior del menor, sin que puedan utilizarse los datos para otros fines, como sería el uso del sistema de videovigilancia con fines de seguridad privada, control laboral exclusivamente o cualesquiera otros.