Expediente Nº: E/02894/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el **EXCMO. C.C.C.** en virtud de denuncia presentada por D. ***B.B.B.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Fecha de entrada de la denuncia: 6 de abril de 2017

Denunciante: D. ***B.B.B.(A.A.A.)***

Denuncia a: ***C.C.C.***

Por los siguientes hechos según manifestaciones del denunciante:

Instalación de cámaras de videovigilancia en diferentes departamentos municipales (.....) situadas delante de los puestos de trabajo con grabación directa de los funcionarios, entendiendo que se realiza de forma desproporcionada.

Todo ello sin información alguna a los trabajadores ni a los representantes sindicales y sin carteles informativos, desconociendo qué personal está autorizado o tiene acceso a las imágenes, que según el modelo de cámara pueden ser visualizadas a través de dispositivos móviles.

Que según el denunciante tuvieron lugar a fecha de: ocurrían en el momento de la denuncia.

Y, entre otra, anexa la siguiente documentación:

> reportaje fotográfico donde se aprecia en su mayoría la existencia de cámaras encima de las mesas de los trabajadores, al lado del equipo informático del puesto de trabajo.

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:

1. Existen dos grupos diferenciados de cámaras:

   Las cámaras de la Casa Consistorial y las de las dependencias de la Policía Local se encuentran conectadas a sistema de grabación y emiten imágenes en directo.

Están instaladas en el interior y el perímetro exterior, estando el acceso a estas últimas concedido exclusivamente a la Policía Local.

> Las cámaras instaladas en otras dependencias municipales (cámaras denunciadas) no tienen sistema de grabación, constando de un sensor de movimiento que cuando se activa puede emitir un correo a las direcciones con seis imágenes y un video con unos segundos de movimiento. Hasta la

fecha no se ha utilizado dicha funcionalidad no estando configurada la cuenta de correo a la que se deben enviar las imágenes, por lo que no existe grabación de imágenes.

Tampoco se encuentra instalado el aplicativo que permite visionar las imágenes en directo.

Respecto a este último grupo de cámaras (cámaras denunciadas) caben las siguientes consideraciones:

2. Se encuentran en su mayoría, según las fotografías aportadas por el denunciante, encima de las mesas de los trabajadores, al lado del equipo informático del puesto de trabajo y con posible captación directa y cercana del trabajador.
3. Declaran que cuando se instalaron no estaban operativas y que **han sido retiradas** físicamente de su ubicación dada la confusión creada, para proceder a instalarlas cuando proceda.
4. La instalación la realizó personal propio del Ayuntamiento.
5. Las cámaras no tienen posibilidad de movimiento ni zoom. No aportan fotografías de las imágenes captadas ni de las cámaras indicando que no están en producción ni físicamente en su ubicación, al haber sido retiradas.
6. La finalidad de la instalación es la vigilancia de las sedes externas municipales, que no cuentan con ningún tipo de vigilancia ni seguridad, además de la protección de los sistemas de fichaje, al haber sufrido sabotaje uno de ellos.
7. Aun no se han ubicado los carteles informativos dado que las cámaras no están puestas en producción.

Respecto a la información facilitada a los trabajadores indican que los representantes de los mismos son conocedores de las medidas ya que el Jefe de Servicio de RRHH las ha expuesto a éstos en la Mesa Técnica de Trabajo delegada de la Mesa General de Negociación, declarando que, no obstante, previamente al inicio del funcionamiento del sistema, se comunicara a todos los trabajadores, además de a sus representantes.

8. No hay sistemas de monitorización instalados.
9. El código de inscripción del fichero de videovigilancia en el Registro General de Protección de Datos de esta Agencia es el ***D.D.D.***, que prevé la videovigilancia de la casa consistorial y el resto de inmuebles municipales.

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 los 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 caso que nos ocupa, D. ***B.B.B. (A.A.A.)*** denuncia instalación de cámaras de videovigilancia en diferentes departamentos municipales del ***C.C.C.*** (.....) situadas delante de los puestos de trabajo, con grabación directa de los funcionarios, entendiendo que se realiza de forma desproporcionada. Todo ello sin información alguna a los trabajadores ni a los representantes sindicales y sin carteles informativos, desconociendo qué personal está autorizado o tiene acceso a las imágenes, que según el modelo de cámara pueden ser visualizadas a través de dispositivos móviles.

Ante dicha denuncia, la Inspección de Datos de esta Agencia solicita información a la entidad denunciada, para el esclarecimiento de los hechos denunciados, manifestando ésta que las cámaras denunciadas instaladas en varias dependencias municipales (instalaciones deportivas, cementerios, mercados…) no tienen sistema de grabación, constando de un sensor de movimiento que cuando se activa puede emitir un correo a las direcciones con seis imágenes y un video con unos segundos de movimiento. Hasta la fecha no se ha utilizado dicha funcionalidad no estando configurada la cuenta de correo a la que se deben enviar las imágenes, por lo que no existe grabación ni imágen alguna de las dependencias municipales. Tampoco se encuentra instalado el aplicativo que permite visionar las imágenes en directo. Declaran que cuando se instalaron no estaban operativas y que han sido retiradas físicamente de su ubicación dada la confusión creada, para proceder a instalarlas cuando proceda.

Dado que las cámaras han sido retiradas y no se encontraban todavía en funcionamiento, no han captado imagen de personas físicas identificadas o identificables, al margen de la normativa de protección de datos

En definitiva, el principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y acreditado una prueba de cargo acreditativa de los hechos que motivan esta imputación o de la intervención en los mismos del presunto infractor.

En el presente caso, al haber sido retiradas las cámaras que aún no estaban operativas, no se ha acreditado la captación o grabación de imágenes de datos personales

por parte de la denunciada, contraviniendo la normativa de protección de datos, por lo que procede el archivo del presente expediente de actuaciones previas.

No obstante, y dado que las cámaras denunciadas se encuentraban en su mayoría, según las fotografías aportadas por el denunciante, encima de las mesas de los trabajadores, al lado del equipo informático del puesto de trabajo y con posible captación directa y cercana del trabajador, debe realizarse una serie de consideraciones respecto a la captación de imágenes en el entorno laboral.

A este respecto, además de los requisitos generales exigidos por la normativa de protección de datos relativos a la información, inscripción del fichero, medidas de seguridad u otras , aquí se plantearía la cuestión de la proporcionalidad en la instalación de las cámaras denunciadas, en la forma en la que se había realizado.

En este sentido es especialmente clarificador y a tener en cuenta, por el citado Ayuntamiento, respecto al concepto de proporcionalidad en el entorno de trabajo, el informe del gabinete jurídico de esta Agencia número 0475/2014, en respuesta a una consulta realizada en las que se plantea el control laboral de trabajadores de un centro de educación infantil y que a continuación se transcribe en la parte que afecta al control laboral: << (…)

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 dela 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 eñala 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 ene stos 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 amparo10522/2009, 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 dela 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 lostrabajadores 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 (WP48), 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 3ªde 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.>>

Por lo tanto, a la vista del informe transcrito, el Ayuntamiento tendrá que tener en cuenta las consideraciones establecidas en el mismo, a la hora de la instalación de un sistema de videovigilancia para el control laboral, procediendo el archivo del presente expediente por los motivos ya citados.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **EXCMO. C.C.C.** y D. ***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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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