N/REF: 017583/2016

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 videovigilancia implantado por la consultante, en particular "*si cuando la cámara instalada en una de esas 50 taquillas, con el fin de proteger la seguridad, visualiza y graba a la persona del trabajador que se encuentra en dicho lugar, no protegido por el derecho a la intimidad, ¿se está excediendo la finalidad de seguridad a la que está destinada?*". Comenzaremos haciendo unas consideraciones genéricas sobre la protección de datos personales en lo que atañe a la utilización de cámaras que capten imágenes de personas para después estudiar el supuesto concretamente planteado.

I

En primer lugar, en el sitio web de esta Agencia se encuentra disponible una Guía sobre videovigilancia que será próximamente revisada y actualizada. Debemos partir de la consideración de que la imagen de la persona es un dato personal, y su tratamiento derivado de la captación y, en su caso, grabación, ha de ajustarse a la normativa sobre protección de datos de carácter personal.

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.

En el ámbito de la videovigilancia, el fin más comúnmente perseguido es el de la seguridad de las personas y las propiedades. En este caso, la legitimación puede venir determinada por el interés legítimo, en el sentido de que el tratamiento sea necesario para satisfacer un interés legítimo perseguido por el responsable del tratamiento y siempre que no prevalezcan los derechos o libertades fundamentales del titular de los datos. Es decir, cuando se persiguen con el sistema de videovigilancia fines relacionados con la seguridad privada de personas, de bienes e instalaciones, con el fin de evitar robos o vandalismo, o en general proteger el patrimonio o las personas, puede entenderse que concurre un interés legítimo, siempre que tales sistemas

- Se instalen en lugares necesarios para cumplir tales fines de seguridad privada

- Mediante las cámaras necesarias para ello

- Siempre que la finalidad de videovigilancia no pueda obtenerse por otros medios que, sin exigir esfuerzos desproporcionados, resulten menos

intrusivos para la intimidad de las personas y para su derecho a la protección de datos

- Y con el establecimiento de las salvaguardias necesarias establecidas en la Instrucción 1/2006:
    - Cumpliendo el deber de información previsto en el artículo 5 de la LOPD y en particular colocando al menos un distintivo informativo en lugar suficientemente visible y teniendo a disposición de los interesados impresos en los que se detalle la información prevista en dicho artículo.
    - No captando imágenes de las vías públicas salvo, en su caso, en el espacio estrictamente necesario
    - Cumpliendo el principio de proporcionalidad Permitiendo en todo caso el ejercicio de los derechos de acceso, rectificación, cancelación y oposición
    - Observando las medidas adecuadas de seguridad y secreto

Ahora bien, los sistemas de videovigilancia también pueden perseguir otros fines, como puede ser el control laboral de los trabajadores, que 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.

Sin embargo, recientemente la Sentencia del Pleno del Tribunal Constitucional de 3 marzo 2016, recurso de amparo 7222/2013 ha modulado las afirmaciones anteriores, al indicar que el sistema de videovigilancia con fines de control laboral, al aparecer amparado en el art. 20.3 ET en relación con el art. 6.2 LOPD, no requiere del consentimiento del trabajador, pero además el deber de información al trabajador puede entenderse cumplimentado con la utilización de los genéricos distintivos informativos en lugar suficientemente visible y teniendo a disposición de los interesados impresos en los que se detalle la información prevista en el art. 5. Señala la citada sentencia:

"Aplicando la doctrina expuesta al tratamiento de datos obtenidos por la instalación de cámaras de videovigilancia en el lugar de trabajo, que es el problema planteado en el presente recurso de amparo, debemos concluir que el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art. 20.3 TRLET , que establece 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". Si la dispensa del consentimiento prevista en el art. 6 LOPD se refiere a los datos necesarios para el mantenimiento y el

cumplimiento de la relación laboral, la excepción abarca sin duda el tratamiento de datos personales obtenidos por el empresario para velar por el cumplimiento de las obligaciones derivadas del contrato de trabajo. El consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario.

En definitiva, la exigencia de finalidad legítima en el tratamiento de datos prevista en el art. 4.1 LOPD viene dada, en el ámbito de la videovigilancia laboral, por las facultades de control empresarial que reconoce el art. 20.3 TRLET, siempre que esas facultades se ejerzan dentro de su ámbito legal y no lesionen los derechos fundamentales del trabajador".

Incide sin embargo dicha resolución en la necesaria observancia del principio de proporcionalidad: *"Por ello, como hemos señalado, aunque no se requiere el consentimiento expreso de los trabajadores para adoptar esta medida de vigilancia que implica el tratamiento de datos, persiste el deber de información del art. 5 LOPD. Sin perjuicio de las eventuales sanciones legales que pudieran derivar, para que el incumplimiento de este deber por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad. Debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el art. 20.3 TRLET, en conexión con los arts. 33 y 38 CE. En efecto, la relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso de los derechos y bienes constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva, que es reflejo de los derechos constitucionales reconocidos en los arts. 33 y 38 CE y que, como se ha visto, en lo que ahora interesa se concreta en la previsión legal ex art. 20.3 TRLET que expresamente faculta al empresario a adoptar medidas de vigilancia y control para verificar el cumplimiento por los trabajadores de sus obligaciones laborales (SSTC 186/2000, de 10 de julio, FJ 5; 170/2013, de 7 de octubre, FJ 3). Esta facultad general de control prevista en la ley legitima el control empresarial del cumplimiento por los trabajadores de sus tareas profesionales (STC 170/2013, de 7 de octubre; STEDH de 12 de enero de 2016, caso Barbulescu v.Rumania), sin perjuicio de que serán las circunstancias de cada caso las que finalmente determinen si dicha fiscalización llevada a cabo por la empresa ha generado o no la vulneración del derecho fundamental en juego".*

II

Ahora bien, como hemos reiterado en varias ocasiones, como en el informe 475/2014 disponible en nuestra página web, esto 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, puesto que habrá de observarse el 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. En el informe aludido 475/2014

contemplábamos una serie de criterios, extraídos tanto de informes del Grupo de Berlín, como del 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 particular en su Dictamen 8/2001 (WP 48), sobre el tratamiento de datos personales en el contexto laboral, así como en el Documento de Trabajo de 29 de mayo de 2002 (WP 55), relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo en el que se examina la vigilancia por el empleador de la utilización del correo electrónico e Internet por parte de los trabajadores; y finalmente de 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.

Con carácter general, esta Agencia entiende que si bien cabe la captación de imágenes de los trabajadores con fines de control laboral, ello no puede realizarse de modo que suponga una monitorización constante y completa de los trabajadores. De este modo, si bien cabe la captación de imágenes en el lugar de efectiva prestación de servicios por el empleado, excluyendo los lugares no destinados a tal fin, como vestuarios u habitaciones, comedores o lugares de descanso, la finalidad ha de ser el control por el empresario en el lugar de trabajo, pero no cabe una monitorización del trabajador durante toda su jornada en el lugar de trabajo que supondría una medida intrusiva y probablemente desproporcionada en relación con la finalidad perseguida, sin ser una respuesta proporcionada ante riesgos potenciales o concretos.

Rescatamos la mención al Documento de Trabajo de 29.5.2002 citado, que señala al respecto que *"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)."*

O en el informe del grupo de Berlín de agosto de 1996 que critica la monitorización continua, porque la información sobre la actuación o el comportamiento personal de los trabajadores puede ser recopilada y utilizada.

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.

O en palabras del Dictamen 8/2001, en el apartado 12 específicamente destinado a vigilancia y monitorización (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.

Como afirmábamos en el reiterado informe 475/2014, "*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".*

III

Una vez estudiado el principio de proporcionalidad en su aplicación a la utilización de cámaras con fines de control laboral, debemos estudiar si la implantación de un sistema que, por sí mismo no tiene fines de control laboral, sino de seguridad, pero que al implantarse puede suponer una monitorización de la actividad del trabajador, supone la lesión a la normativa que nos ocupa.

Parece que la cuestión aparece directamente solucionada en la ya citada **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, que parte de 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. 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".*

Esto supone que, por un lado, siempre que sea posible las cámaras sobre las taquillas sean instaladas de forma que no capten al trabajador, y que no lo hagan permanentemente. Puesto que su finalidad es eminentemente de seguridad, entendemos que en aquellas taquillas en las que sea posible así se hará.

Y, en segundo lugar, si ello no es posible, habrá que estudiar las circunstancias de cada caso concreto; sin embargo con carácter abstracto podemos decir, por un lado, que esta circunstancia no debería afectar a la finalidad perseguida por el responsable del tratamiento, puesto que es él el que decide dicha finalidad. Esta circunstancia afectaría a la proporcionalidad y a la posibilidad de adoptar otros medios menos invasivos. Y si la finalidad perseguida por el sistema de captación y en su caso grabación de imágenes es de seguridad, y ello supone indirectamente la monitorización de los trabajadores, cabría su uso, si bien implantando el sistema con la previa información a los trabajadores, indicando expresamente que no tienen una finalidad de control laboral y que las imágenes no podrán ser utilizadas para tal fin, y estableciendo las salvaguardas que se estimen necesarias. Por ejemplo, imponiendo ulteriores medidas de seguridad, como en lo que afecta al acceso a las imágenes, clarificando que no podrá ser realizado por el empresario – en este caso, el personal de recursos humanos, o el superior jerárquico del empleado – con fines de control laboral de los trabajadores. Podría también indicarse así en los distintivos, si se estima necesario. Y en cualquier caso observarse las precisiones de la Instrucción 1/2006, sin exceder de los plazos

de cancelación en ella previstos bajo la excusa de conservar las imágenes para otros fines que excedan de la videovigilancia para seguridad. Es decir, la empresa podría adoptar mecanismos internos que determinaran que las imágenes en ningún caso serán utilizadas con fines de control laboral, sino para las finalidades previstas del fichero en cuestión, implantando una serie de medidas que garantizaran que así se realizará.