



La presente consulta plantea si es conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, cuestiones tales como el control control de la actividad laboral con cámaras de videovigilancia, el cumplimiento del deber de información y el personal autorizado para el visionado de las imágenes grabadas en un sistema de videovigilancia en un aeropuerto con fines de seguridad.

I

Sobre las cuestiones relativas a la posibilidad de utilizar sistemas de videovigilancia con fines de control laboral se ha pronunciado en varias ocasiones esta Agencia y cabe citar, entre otros, el Informe 0475/2014 disponible en nuestra página web.

En todo caso, al objeto de afrontar las consulta, 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 de la Ley 15/1999, 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 Ley, 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) Reglamento de desarrollo de la Ley, 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 Ley 15/1999 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.

Partiendo de este principio general, la vigilancia por videocámaras puede estar justificada en determinadas circunstancias, sin embargo, se hace necesario adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos de manera que el tratamiento de imágenes con fines de videovigilancia sea adecuado a los principios de la Ley Orgánica 15/1999 y garantizar así los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos.

A este respecto la citada Instrucción 1/2006, remite en su artículo 2 a lo previsto en el artículo 6.1 y 2 de la Ley Orgánica 15/1999, donde se establece que *“el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”*, sin perjuicio de que dicho consentimiento podrá quedar excluido, de acuerdo con lo dispuesto por el artículo 6.2 cuando, el tratamiento sea necesario para el adecuado desenvolvimiento de la relación laboral de los trabajadores con la empresa.

El artículo 20.3 del Texto Refundido del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015 de 23 de octubre, 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. 6.2 de la Ley 15/1999, legitimaría, en principio, a la empresa 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 Ley 15/1999, 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 Ley 15/1999). 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”*

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 Ley 15/1999, incluyendo en todo caso la previa información a los trabajadores y a sus representantes.

Sin embargo, 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”.

Ahora bien, 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, que quepa todo tratamiento de datos amparado en dicha finalidad.

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.

En el presente caso, y sobre la base de los datos planteados por la consulta, cabe responder que el sistema de videovigilancia que ya se encuentra instalado para fines de seguridad, puede utilizarse verificar el cumplimiento de la actividad que desempeñan los vigilantes de seguridad en los puestos que tengan asignados siempre y cuando, no suponga una monitorización constante de los trabajadores durante la totalidad de su jornada laboral, sino en unos ámbitos y momentos concretos y determinados relacionados con el interés legítimo de la empresa.

II

Respecto a la necesidad de informar a los trabajadores sobre la instalación de cámaras de videovigilancia, sin perjuicio de lo señalada en el primer apartado de este informe sobre la legitimidad de la medida, baste recordar lo establecido en la Instrucción 1/2006, de 8 de noviembre, sobre tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, cuyo artículo 3 dispone que.



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

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

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

En consecuencia, sería posible dar cumplimiento a lo dispuesto en el artículo 5.1 de la Ley Orgánica 15/1999 mediante la colocación de un cartel informativo que contuviera los extremos previstos en dicho precepto.

III

Respecto a la cuestión relativa al visionado de las cámaras de seguridad, es preciso indicar que la competencia de la Agencia Española de Protección en relación con la aplicación de la Ley 5/2014, de 4 de abril, de Seguridad Privada, ha de limitarse al análisis del tratamiento que justifica la instalación de las cámaras y si el mismo se encontraría legitimado por lo dispuesto en la Ley Orgánica 15/1999 sin exigir para ello que las imágenes sean visualizadas directamente por una empresa de seguridad privada.

Teniendo en cuenta esta premisa, es preciso indicar que el tratamiento de datos con fines de videovigilancia efectivamente aparece regulado expresamente en el artículo 42 de la Ley 5/2014. En particular, el párrafo segundo del apartado 1 de dicho precepto señala que “cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales”.

No obstante, la interpretación del mencionado precepto debe llevarse a cabo a la luz del texto íntegro de la propia Ley 5/2014, de forma que el alcance del citado artículo 42 será el que se derive de lo que dispone la Ley en cuanto a la determinación de su ámbito de aplicación y, particularmente, de las actividades incluidas y excluidas de la misma a las que se refieren sus artículo 5 y 6.



En este sentido, el artículo 5.1, en sus apartados f) y g) considera actividades de seguridad privada “la instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia” y “la explotación de centrales para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma, así como la monitorización de cualesquiera señales de dispositivos auxiliares para la seguridad de personas, de bienes muebles o inmuebles o de cumplimiento de medidas impuestas, y la comunicación a las Fuerzas y Cuerpos de Seguridad competentes en estos casos”.

Por su parte, el artículo 6 se refiere en sus dos primeros apartados a una serie de actividades de seguridad que quedan fuera del ámbito de aplicación de la Ley, aun cuando es posible que las mismas puedan llevarse a cabo por empresas dedicadas a la seguridad privada, de forma directa o complementaria y sin que dicha normativa resulte de aplicación en tal caso.

Entre tales actividades, la letra b) del apartado 1 se refiere a “la fabricación, comercialización, venta o entrega de equipos técnicos de seguridad electrónica, así como la instalación o mantenimiento de dichos equipos siempre que no estén conectados a centrales de alarma o centros de control o de videovigilancia”.

De ello se desprendería que el criterio relativo a la existencia de libre competencia en la prestación del servicio derivado de lo dispuesto en la Ley 25/2009, de 22 de diciembre, de Modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio no se ha visto modificado por la entrada en vigor de la Ley 5/2014.

La consecuencia de lo anterior es que el criterio sustentado por esta Agencia como consecuencia de la entrada en vigor de la Ley 25/2009 no se ha visto alterado a su vez por la entrada en vigor de la Ley 5/2014. De este modo, la intervención de una empresa de seguridad privada únicamente sería exigible para el tratamiento de datos relacionado con la videovigilancia en caso de que aquél se encontrase conectado a una central de alarmas.

IV

Por último señalar que, si el sistema de videovigilancia ya está instalado y por lo tanto existe, y que aunque se quiera usar para unas finalidades



adicionales a las propias de la vigilancia de personas y bienes (esto es, se pretende usar también para finalidades de control laboral) el tratamiento de datos en que consiste la videovigilancia habrá de cumplir con lo establecido en la normativa aplicable. Ello incluye, ciertamente, la Instrucción 1/2006, de 8 de noviembre de esta Agencia sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Y además, si como hemos concluido en anteriores apartados, dicho sistema de videovigilancia puede utilizarse para fines de control laboral. En todo caso, cuando las cámaras se utilicen con fines de control laboral y de seguridad, en la inscripción del fichero se hará constar la doble finalidad.