



La consulta plantea si es posible la utilización para el control de personal del sistema de videovigilancia que ya está instalado para fines de seguridad pública en la zona interior de entrada de sus sedes, y en caso afirmativo, cuestiona sobre el plazo de cancelación de dichos datos en relación con el plazo de un mes previsto en el artículo 6 de la Instrucción 1/2006 de 8 de noviembre de la Agencia Española de Protección de Datos (AEPD).

I

Sobre la primera cuestión planteada, es decir, sobre la posibilidad de utilizar con fines de control laboral el sistema de videovigilancia instalado para otros fines, se ha pronunciado en varias ocasiones esta AEPD. Cabe citar, entre otros, el Informe mencionado por la solicitante en su consulta, 0475/2014.

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:
 - o 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.
 - o No captando imágenes de las vías públicas salvo, en su caso, en el espacio estrictamente necesario.
 - o Cumpliendo el principio de proporcionalidad permitiendo en todo caso el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
 - o 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, la Sentencia 39/2016 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 (STC 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, como hemos reiterado en varias ocasiones, como en el informe 475/2014 reiterado, 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.

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 Tribunal de Cuentas puede utilizar para el control del cumplimiento del horario del personal a su servicio el sistema de videovigilancia que ya se encuentra instalado para fines de seguridad pública en la zona interior de entrada de sus sedes, habida cuenta que se considera que el mismo no supone 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 del solicitante de



verificar el cumplimiento de los horarios de trabajo y control de presencia. Y ello además siempre que se cumpla con el principio de información, en los términos expuestos.

II

Respecto de la segunda de las cuestiones, cabe partir para su análisis de un hecho concreto que es el que se ha tenido en cuenta para responder a la primera pregunta, y es que 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 la AEPD 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 el apartado anterior, dicho sistema de videovigilancia puede utilizarse para fines de control laboral, en caso de utilización de datos concretos para dicho fin, el tratamiento de dichos datos habrá de cumplir igualmente, también, los requisitos relativos al fichero que se concrete dicha finalidad.

En lo que respecta al principio de conservación de los datos debe recordarse que el artículo 4.5 de la Ley 15/1999 establece que *“Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.”*

No obstante, en el caso de la videovigilancia, el artículo 6 de 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, concreta dicho plazo fijándolo en un mes como máximo desde la captación de las imágenes.

Debe, además, tomarse en consideración que la cancelación de los datos no supone automáticamente el borrado o supresión físico de los datos, sino su bloqueo, tal y como dispone el artículo 16.3 de la Ley Orgánica 15/1999

según el cual *“la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”*.

El Reglamento de desarrollo de la Ley Orgánica 15/1999, precisa el concepto al definir la cancelación en su artículo 5.1.b) como el *“Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.”*

Así, el plazo de conservación de las imágenes en el fichero de videovigilancia será con carácter general de un mes como máximo, y dicha norma no establece excepciones. Y ello sin perjuicio de que aunque en el plazo de un mes haya de procederse a bloquear dichos datos (las imágenes), hayan de conservarse las mismas para su puesta a disposición de las administraciones públicas, jueces y tribunales, en la forma que establece el ya citado art. 5.1.b) RLOPD.

Ahora bien, el ámbito objetivo de aplicación de la Instrucción 1/2006, de 8 de noviembre, se contiene en el artículo 1 de la misma, y dicho artículo hace referencia a que esta Instrucción se aplica al tratamiento de los datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistema de cámaras y videocámaras.

Por lo tanto, dicha Instrucción no hace referencia al uso de dichos datos cuando se utilicen para una finalidad legítima diferente de la “vigilancia”, como por ejemplo el “control laboral”. Y si el sistema de videovigilancia puede utilizarse para ambas finalidades el responsable del tratamiento deberá cumplir los requisitos legales establecidos para ambos supuestos.

Aplicando lo anterior al caso presente, cabe entender que, respondiendo a la concreta cuestión planteada por la solicitante, en el caso de que del

estudio de las imágenes resulten circunstancias que permitan apreciar un comportamiento que pudiera dar lugar a un procedimiento disciplinario derivado de los incumplimientos del horario de trabajo establecido u otras circunstancias relacionadas con el control laboral, dichas imágenes concretas y específicas podrán trasladarse, mediante su copiado, al concreto procedimiento que habrá de hacerse constar en un fichero diferente al propio de videovigilancia (por ejemplo, al fichero de gestión del personal) en cuyo caso, dichos datos (las imágenes) seguirán el tratamiento de la normativa propia del fichero al que se incorporan, incluyendo por supuesto los derechos de acceso, rectificación, cancelación y oposición propios del mismo, lo que incluye lo dispuesto en el artículo 4.5 ya citado de la LOPD, que establece, reiteramos, que los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubiera sido recabados por registrados, y dado que la finalidad para la cual dicho dato ha sido registrado en un fichero diferente del propio de videovigilancia es, en este caso, de control laboral, dicho dato podrá ser conservado hasta que ya no sea necesario o pertinente para dicha finalidad de control laboral.

Se hace la precisión de que se trasladen mediante copia dichos datos para no atentar contra la integridad del fichero de videovigilancia (art. 4.4 LOPD), el cual habrá de contener la totalidad de los datos que se hayan registrado con dicha finalidad de videovigilancia, para que los mismos puedan estar a disposición de los Tribunales de Justicia o de la Administración Pública en los términos previstos por el propio artículo 5.1.b) RLOPD)

Ha de hacerse mención también, brevemente apuntada con anterioridad, a que dicho traslado de datos del sistema de videovigilancia a un fichero diferente habrá de cumplir igualmente con los principios de calidad de los datos contenidos en el artículo 4 LOPD, de manera que dicho tratamiento de datos ha de ser en todo caso adecuado, pertinente y no excesivo en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido o registrado. Por ello, hay que recalcar que los datos que podrán reflejarse en el fichero de control laboral habrán de ser exclusivamente los adecuados, pertinentes y no excesivos, lo que en el caso concreto conlleva que sólo podrán reflejarse en el fichero de control laboral imágenes específicas y concretas relativas a la infracción observada en materia control de presencia y en ningún caso la totalidad de las imágenes que consten en el fichero de videovigilancia, pues este tratamiento de imágenes en las que no se haya



observado ninguna irregularidad no se considera ni adecuado ni pertinente, siendo excesivo por tanto a la finalidad de control laboral para la que se autoriza el tratamiento.