DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 21 | Marzo 2022

LA VIDEOVIGILANCIA EN EL ENTORNO LABORAL

Í N D I C E

LA VIDEOVIGILANCIA EN EL ENTORNO LABORAL

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"LA INSTALACIÓN DE VIDEOCÁMARAS CON FINALIDAD DE CONTROL LABORAL SUPONE UN TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL Y, EN CONSECUENCIA, RESULTA DE APLICACIÓN LA NORMATIVA DE PROTECCIÓN DE DATOS".

INTRODUCCIÓN

La imagen de una persona es un dato personal, ya que identifica o hace identificable a la misma. En este sentido, la instalación de videocámaras con finalidades como la seguridad o el control laboral supone un tratamiento de datos de carácter personal y, en consecuencia, resulta de aplicación la normativa de protección de datos. No sólo eso, sino que en la instalación de este tipo de dispositivos también entra en juego el derecho a la intimidad y la propia imagen de aquellas personas cuyas imágenes son captadas (artículo 18 de la Constitución Española y desarrollado por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen).

No obstante, estos derechos se contraponen con otro establecido en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET), que en su artículo 20.3 faculta al empleador a adoptar las medidas de vigilancia y control que estime más oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. También las entidades públicas podrían ejercer tal control cuando tuviera como finalidad verificar el cumplimiento por parte de los trabajadores de sus obligaciones laborales, en base al artículo 54 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público (EBEP).

Aunque no es una cuestión pacífica, tanto la legislación como las autoridades en materia de protección de datos y los Tribunales, a través de su actividad jurisprudencial, han ido proporcionando seguridad jurídica en relación con la instalación de videocámaras con la finalidad de control del cumplimiento de las obligaciones laborales.

LEGITIMACIÓN PARA EL TRATAMIENTO DERIVADO DE LAS VIDEOCÁMARAS CON FINES DE CONTROL LABORAL

Como adelantábamos, los sistemas de videovigilancia con fines de control laboral se encuentran amparados en el artículo 20.3 del ET, que reza:

> *"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".*

Por su parte, el artículo 89 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) regula el derecho a la intimidad frente al uso de dispositivos de videovigilancia en el lugar de trabajo:

> *"1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo".*

"LA BASE JURÍDICA PARA EL CONTROL DE LAS PERSONAS TRABAJADORAS MEDIANTE VIDEOVIGILANCIA ES EL CONTRATO DE TRABAJO Y LAS FACULTADES LEGALES DE CONTROL CONCEDIDAS AL EMPLEADOR, POR LO QUE NO SE REQUIERE EL CONSENTIMIENTO DE LAS PERSONAS TRABAJADORAS".

En definitiva, la base jurídica para el control de las personas trabajadoras mediante videovigilancia es el contrato de trabajo y las facultades de control que la legislación concede al empleador, por lo que no se requiere el consentimiento de las personas trabajadoras.

PROPORCIONALIDAD

La videovigilancia únicamente debe utilizarse cuando no sea posible acudir a otros medios que causen menos impacto en la privacidad. En este sentido, los sistemas de videovigilancia para control empresarial sólo se adoptarán cuando exista una relación de proporcionalidad entre la finalidad perseguida y el modo en que se traten las imágenes y no haya otra medida más idónea.

El control audiovisual ha de respetar los derechos fundamentales de la persona trabajadora, especialmente el derecho a la intimidad personal (STC 98/2000, de 10 abril y 186/2000, de 10 julio).

Por ejemplo, la Agencia Española de Protección de Datos (AEPD), en su Guía "La protección de datos en las relaciones laborales", señala:

Ejemplo.

La tecnología permitiría que a través de la videovigilancia un empresario observe las expresiones faciales de trabajador por medios automatizados, identifique desviaciones con respecto a los patrones de movimiento predefinidos, etc. Esto sería desproporcionado a efectos de los derechos y libertades de los trabajadores y, por tanto, ilícito. El tratamiento también puede implicar la elaboración de perfiles y, posiblemente, la toma de decisiones automatizadas. Por tanto, la videovigilancia no puede utilizarse en combinación con otras tecnologías, como el reconocimiento facial, porque en tal caso el control resulta desproporcionado (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, del Grupo de Trabajo del Artículo 29).

"LA VIDEOVIGILANCIA NO PUEDE UTILIZARSE EN COMBINACIÓN CON OTRAS TECNOLOGÍAS, COMO EL RECONOCIMIENTO FACIAL, PORQUE EN TAL CASO EL CONTROL RESULTA DESPROPORCIONADO".

"SE DEBERÁ INFORMAR A LAS PERSONAS TRABAJADORAS DE LA EXISTENCIA DE UN SISTEMA DE VIDEOVIGILANCIA. LA INFORMACIÓN DEBERÁ SER TRANSMITIDA CON CARÁCTER PREVIO Y DE FORMA EXPRESA, CLARA Y CONCISA, A LOS TRABAJADORES O LOS EMPLEADOS PÚBLICOS Y, EN SU CASO, A SUS REPRESENTANTES".

DEBER DE INFORMACIÓN

En todo caso, se debe informar a las personas trabajadoras de la existencia de un sistema de videovigilancia. A este fin, se debe colocar un cartel suficientemente visible en los accesos a las zonas vigiladas, que indique de forma clara la identidad del responsable del tratamiento, dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos y dónde obtener más información sobre el tratamiento de los datos personales. A esos efectos, se puede utilizar el modelo de cartel puesto a disposición por la AEPD:

Igualmente, se debe poner a disposición de los afectados el resto de la información a la que se refiere el artículo 13 del Reglamento General de Protección de Datos (RGPD).

La información deberá ser transmitida con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes.

"ESTÁ PROHIBIDA LA INSTALACIÓN DE SISTEMAS DE GRABACIÓN DE IMAGEN Y/O SONIDO EN LUGARES DESTINADOS AL DESCANSO O ESPARCIMIENTO DE LAS PERSONAS TRABAJADORAS, TALES COMO VESTUARIOS, ASEOS, COMEDORES Y ANÁLOGOS".

No obstante, la Sentencia del Tribunal Europeo de los Derechos Humanos (STEDH López Ribalda II de 17-10-2019) admite, dadas las circunstancias del caso, que la no advertencia a la persona trabajadora, de forma concreta, sobre el emplazamiento de la cámara, en un supuesto en el que sí ha existido información sobre la instalación de cámaras de videovigilancia y concurre una sospecha fehaciente de incumplimiento grave de las obligaciones laborales (en este caso, sustracción de forma continuada con alto valor económico) no conduce a la nulidad de las pruebas obtenidas para imponer una sanción a la persona trabajadora, pero la empresa puede ser considerada responsable en el ámbito de la protección de datos, por infracción de la obligación de informar, debiendo hacer frente a las responsabilidades civiles y administrativas que se puedan derivar de ese incumplimiento.

PRINCIPIO DE MINIMIZACIÓN

En el ámbito de la videovigilancia, el principio de minimización supone:

- Que el **número de cámaras** se limite a las **necesarias** para cumplir la función de vigilancia.

- Que se analicen también los requisitos técnicos de las cámaras, ya que el ***zoom*, o las cámaras orientables** pueden afectar al citado principio de minimización. En estos casos, podría ser necesaria la instalación de **máscaras de privacidad** para evitar captar imágenes de la vía pública, terrenos, viviendas o cualquier otro espacio ajeno.

Está prohibida la instalación de sistemas de grabación de imagen y/o sonido en lugares destinados al descanso o esparcimiento de las personas trabajadoras, tales como vestuarios, aseos, comedores y análogos. En el Expediente Nº: PS/00337/2021, tramitado por la AEPD, esta sancionó a una empresa por instalar cámaras en la zona donde el personal de seguridad se cambiaba de ropa y almorzaba. Recuerda la AEPD que: *"la instalación de tales medios en áreas de privacidad, como lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos resulta, a fortiori, lesiva en todo caso del*

derecho a la intimidad de los trabajadores, sin más consideraciones, por razones obvias".

"SE DEBEN CONSERVAR LAS IMÁGENES DURANTE UN MES DESDE SU CAPTACIÓN, SALVO CUANDO HUBIERAN DE SER CONSERVADOS PARA ACREDITAR LA COMISIÓN DE ACTOS QUE ATENTEN CONTRA LA INTEGRIDAD DE PERSONAS, BIENES O INSTALACIONES. EN TAL CASO, LAS IMÁGENES DEBERÁN SER PUESTAS A DISPOSICIÓN DE LA AUTORIDAD COMPETENTE EN UN PLAZO MÁXIMO DE SETENTA Y DOS HORAS DESDE QUE SE TUVIERA CONOCIMIENTO DE LA EXISTENCIA DE LA GRABACIÓN".

PAUTAS PARA LA GRABACIÓN Y CONSERVACIÓN DE IMÁGENES

1. Los **monitores de grabación** deben situarse de forma que, en la medida de lo posible, únicamente puedan ser visualizados por aquellos cuya función sea controlar los equipos que realizan las grabaciones. En ningún caso deben estar ubicados de forma que usuarios puedan ver las imágenes.

2. Las **imágenes que se utilicen para denunciar delitos o infracciones** se deben acompañar a la denuncia y conservarse para ser entregadas a las Fuerzas y Cuerpos de Seguridad o a los Juzgados y Tribunales que las requieran. No podrán utilizarse para otro fin.

3. La **petición de imágenes por las Fuerzas y Cuerpos de Seguridad** se debe realizar en el marco de actuaciones judiciales o policiales.

4. Deben implementarse las **medidas de seguridad** pertinentes, en función de los análisis de riesgos y, eventualmente, de la evaluación de impacto si fuera necesaria.

5. Si se encarga a un tercero la gestión de las cámaras, ese tercero tendrá la condición de **encargado del tratamiento** y habrá que regular la relación mediante un contrato de encargo, además de verificar que ofrece garantías suficientes en lo que respecta a la protección de datos y seguridad de la información.

6. Respecto de la **supresión de las imágenes**, el art. 22.3 de la LOPDGDD permite su conservación durante un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

GRABACIÓN DE VOZ EN EL LUGAR DE TRABAJO

El art. 89 de la LOPDGDD limita la utilización de sistemas de grabación de sonidos en el lugar de trabajo, que se admitirá únicamente cuando se acrediten riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando los principios de proporcionalidad y de intervención mínima, así como las garantías indicadas para la videovigilancia.

La AEPD se pronunció al respecto en un Informe publicado a raíz de las dudas planteadas en relación con la instalación de un sistema de videovigilancia con fines de "Seguridad y control de acceso a edificios "y "control de presencia de empleados", que implicaba la captación de imagen y voz de las personas que accedían al edificio y de los trabajadores de corporación. Desde la entidad consultante (un Ayuntamiento) se cuestionaba si debían ser atendidas las alegaciones realizadas por parte de algunos empleados, que consideraban la grabación de voz una vulneración del artículo 18.3 y 4 de la Constitución.

Precisa la AEPD, en primer lugar, que la voz de una persona es un dato personal, al igual que lo es cualquier información que permita determinar, directa o indirectamente, su identidad, por lo que la grabación del sonido de voz en un soporte informatizado constituye un tratamiento o de datos personales.

Se remite después a la Sentencia del Tribunal Constitucional 98/2000, que censura la decisión de una empresa de instalar micrófonos en las zonas de caja y de ruleta francesa que permitían grabar las conversaciones en esas zonas con el objetivo de reforzar la seguridad del casino y poder resolver mejor las eventuales reclamaciones de los clientes. A juicio del Tribunal *"la implantación del sistema de audición y grabación no ha sido en este caso conforme con los principios de proporcionalidad e intervención mínima que rigen la*

"LA VOZ DE UNA PERSONA ES UN DATO PERSONAL, AL IGUAL QUE LO ES CUALQUIER INFORMACIÓN QUE PERMITA DETERMINAR, DIRECTA O INDIRECTAMENTE, SU IDENTIDAD, POR LO QUE LA GRABACIÓN DEL SONIDO DE VOZ EN UN SOPORTE INFORMATIZADO CONSTITUYE UN TRATAMIENTO O DE DATOS PERSONALES".

"LA UTILIZACIÓN DEL SISTEMA DE VIDEOVIGILANCIA PARA GRABAR LAS CONVERSACIONES, TANTO DE EMPLEADOS COMO DE PÚBLICO EN GENERAL, EN LA MEDIDA QUE EL SISTEMA VA A PERMITIR CAPTAR COMENTARIOS PRIVADOS, PUEDE RESULTAR INCOMPATIBLE CON EL PRINCIPIO DE PROPORCIONALIDAD".

modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial, pues la finalidad que se persigue (dar un plus de seguridad, especialmente ante eventuales reclamaciones de los clientes) resulta desproporcionada para el sacrificio que implica del derecho a la intimidad de los trabajadores (e incluso de los clientes del casino). Este sistema permite captar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios ajenos por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por la empresa. Se trata, en suma, de una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE, pues no existe argumento definitivo que autorice a la empresa a escuchar y grabar las conversaciones privadas que los trabajadores del casino mantengan entre sí o con los clientes". (FJ 9).

Atendiendo a la doctrina descrita, considera la AEPD que la utilización del sistema de videovigilancia para grabar las conversaciones de voz, tanto de empleados como de público en general, en la medida que el sistema va a permitir captar comentarios privados, puede resultar incompatible con el principio de proporcionalidad al que nos hemos venido refiriendo.

MATERIAL COMPLEMENTARIO

- Dictamen 2/2017, sobre el tratamiento de datos en el trabajo (GT29). Consulta este enlace.
- Guía: 'Protección de datos en las relaciones laborales' (AEPD). Consulta este enlace.
- Ficha práctica de videovigilancia: 'Cámaras para el control laboral'. Consulta este enlace.
- Sentencia del Tribunal Europeo de los Derechos Humanos (STEDH López Ribalda II de 17-10-2019). Consulta este enlace.
- Resolución Expediente Nº: PS/00337/2021 sobre cámaras en vestuarios (AEPD). Consulta este enlace.
- Informe sobre proporcionalidad en grabación de imágenes de voz de empleados (AEPD). Consulta este enlace.

NOTICIAS

- **La AEPD archiva actuaciones en relación con una entidad que tomaba la temperatura a sus clientes para poder acceder al establecimiento.** El reclamante expone que en la empresa donde ha revisado su vehículo le han tomado la temperatura con un termómetro láser para poder acceder, considerando que se ha vulnerado su derecho a la intimidad y a la protección de datos. La toma de temperatura no conlleva ningún registro ni temporal ni definitivo. Consulta la Resolución en este enlace.

- **La AEPD archiva actuaciones contra un centro educativo por la brecha de seguridad ocasionada por el acceso a los exámenes y módulos del tutor en el aplicativo por parte de los alumnos.** Las actuaciones de inspección se iniciaron por la recepción de un escrito de notificación de brecha de seguridad remitido por el centro educativo en el que informaban a la AEPD que un estudiante había obtenido, mediante observación visual, el código de usuario y la contraseña de un tutor del Centro y había tenido acceso a los exámenes y todos los módulos del tutor. No obstante, la AEPD acredita que la actuación del responsable del tratamiento fue acorde con la normativa sobre protección de datos personales. Consulta la Resolución en este enlace.

- **La APDCAT emite un Dictamen en relación con el uso de dispositivos de control de presencia en el puesto de trabajo mediante reconocimiento facial.** Se presenta ante la APDCAT una consulta de un Ayuntamiento en la que expone que tiene intención de instalar un sistema de control de presencia en el puesto de trabajo mediante reconocimiento facial. El Ayuntamiento solicita conocer la conformidad a la normativa de protección de datos del uso de estos sistemas, y plantea *"[...] qué tratamiento es necesario dar a los datos de reconocimiento facial necesarios para el correcto funcionamiento del aplicativo, y qué pasos debería seguir el Ayuntamiento para poder ponerlo en marcha [...]"*. Consulta el Dictamen en este enlace.