

**Fernando Sánchez Ferrándiz**

Experto en Compliance Penal y Protección de Datos y responsable del Departamento Procesal en Sebastián Abogados y Economistas



Control laboral y privacidad: políticas de videovigilancia y protección de datos

En el ámbito laboral, la videovigilancia se ha convertido en una herramienta comúnmente utilizada por los empleadores que permite garantizar la seguridad de las instalaciones, proteger la propiedad intelectual y física de la empresa, y supervisar el cumplimiento de las obligaciones laborales a cargo de los trabajadores. Sin embargo, la utilización de sistemas de videovigilancia en el lugar de trabajo debe realizarse respetando el derecho a la privacidad de los empleados y siempre de conformidad con la normativa de protección de datos vigente.

En España, el marco normativo que regula estas prácticas incluye el Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), así como la Ley de Prevención de Riesgos Laborales y la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo en materia de derechos fundamentales de los trabajadores. Es importante, también, la observancia de las guías publicadas por la Agencia Española de Protección de Datos (AEPD), organismo público encargado de velar por el cumplimiento de la normativa en materia de protección de datos en España.

La videovigilancia en el trabajo no puede ser ilimitada y debe sujetarse a principios de proporcionalidad, necesidad y minimización de datos, asegurando que se respeten los derechos fundamentales de los trabajadores y se proteja su dignidad en el entorno laboral.

Marco legal aplicable

- **Reglamento General de Protección de Datos (RGPD):** es aplicable directamente en todos los estados miembros de la Unión Europea.
- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD):** adapta el ordenamiento jurídico español al RGPD y desarrolla sus disposiciones, incluyendo aspectos específicos relacionados con la videovigilancia en el trabajo.
- **Estatuto de los Trabajadores (ET):** su artículo 20.3 establece el derecho a la intimidad y a la propia imagen de los trabajadores, lo que limita la instalación de sistemas de videovigilancia en los lugares de trabajo.
- **Ley 5/2014, de 4 de abril, de Seguridad Privada:** regula la instalación y uso de cámaras y sistemas de videovigilancia por parte de empresas de seguridad privada, así como su conexión con las Fuerzas y Cuerpos de Seguridad.
- **Sentencias del Tribunal Supremo y del Tribunal Constitucional:** interpretan y concretan la aplicación de los derechos fundamentales en relación con la videovigilancia en el trabajo.
- **Instrucciones de la Agencia Española de Protección de Datos (AEPD):** emite guías e instrucciones para facilitar la aplicación de la normativa de protección de datos en el contexto de la videovigilancia.

(Imagen: E&J)

Principios de Protección de Datos en la videovigilancia laboral

Base legal o legitimación del tratamiento

Debe tener una base legal clara, como puede ser el consentimiento del interesado, el cumplimiento de una obligación legal o el interés legítimo del responsable.

La LOPDGDD (art. 89) establece que 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 ET 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 AEPD[\[1\]](#) establece lo siguiente al respecto:

1. el ET faculta al empresario para adoptar las medidas que estime más oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, que deberán guardar la consideración debida a la dignidad humana y tener en cuenta la capacidad real de los trabajadores con discapacidad;
2. 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;

3. y se tendrá en cuenta el derecho a la intimidad y a la propia imagen de los trabajadores.

El propio RGPD (art. 22), al tratar los tratamientos con fines de videovigilancia, considera que “las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.”

Principio de lealtad y transparencia. Derecho de información

El tratamiento de datos no debe ser sólo legal, sino también leal, e implícito en dicho deber de lealtad se encuentra el de prestar una información adecuada al afectado o interesado, de forma que conozca el alcance real del consentimiento que presta o, en caso de no precisarse, los fines de la recogida y el modo de ejercitar los derechos.

En todos los casos se deberá informar de la existencia de un sistema de videovigilancia. A este fin se colocará un cartel suficientemente visible en los accesos a las zonas vigiladas, que indicará de forma clara la identidad del responsable de la instalación, ante quién y 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.

También habrá de informarse personalmente a los trabajadores y a la representación sindical, por cualquier medio que garantice la recepción de la información.

Principio de proporcionalidad

Con carácter previo a la instalación de un sistema de videovigilancia, el responsable del tratamiento debe ponderar los bienes jurídicos protegidos, es decir, analizar si no es posible alcanzar el fin perseguido mediante la adopción de medios alternativos que sean menos intrusivos para la protección de datos de carácter personal.

Principio de limitación de la finalidad y minimización: utilización y lugar de instalación

Podrán recabarse las imágenes siempre que su finalidad sea: (i) determinada (no pueden ser finalidades genéricas); (ii) explícita (el tratamiento no puede tener finalidades confusas); (iii) legítima (conforme a Derecho) y (iv) que el afectado haya prestado su consentimiento para el tratamiento de sus datos con esa finalidad. Y, naturalmente, la concurrencia de estos requisitos habrá de mantenerse en el tiempo, no siendo posible usarse, en un momento posterior, con una finalidad distinta de aquella que habría amparado su recogida.

Es necesario, en todo caso, diferenciar los efectos *ad intra* y *ad extra* de este principio de minimización en el

tratamiento de imágenes y su interrelación con el principio de proporcionalidad.

En cuanto a las limitaciones *ad intra*, es decir, que afectan al lugar de trabajo y a las personas que se encuentran en él, se ha de cumplir con el principio de minimización y de proporcionalidad. Por ello, en el caso que nos ocupa, **las cámaras sólo captarán imágenes de los espacios indispensables para el control laboral. En ningún caso se ubicarán en zonas de vestuarios, aseos, comedores y espacios de descanso de los trabajadores.**

Con respecto a la grabación de sonidos en el lugar de trabajo, se admite únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, los bienes y las personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores; límites que reducen drásticamente los casos en que podrá utilizarse la grabación de sonido.

En cuanto a los límites *ad extra* de este principio, el cual se ha de poner en relación con el principio de proporcionalidad, es importante que las cámaras no capten imágenes de la vía pública o propiedades privadas, es decir, captación de imágenes externas al lugar de trabajo y sus exteriores. Si se utilizan cámaras orientables y/o con zoom, será necesaria la instalación de “máscaras” de privacidad para evitar captar imágenes de la vía pública, terrenos, viviendas o cualquier otro espacio ajeno.

Muy clarificadora ha sido la Audiencia Nacional al respecto^[2]. La Sala de lo Contencioso desestima el recurso contra la resolución de la AEPD, teniendo en cuenta que el hecho de que un sistema de videovigilancia haya podido ser instalado conforme a la normativa de seguridad, no autoriza a realizar grabaciones de imágenes en la vía pública más allá de lo que resulta idóneo, adecuado y proporcional.

(Imagen: E&J)

Control del sistema de grabación y visualización de imágenes. Medidas de seguridad y supresión. Problemática existente

Es menester, en este punto, enumerar las medidas necesarias para un adecuado control del sistema de videovigilancia:

1. el sistema de grabación se ubicará en un lugar vigilado o de acceso restringido;
2. a las imágenes grabadas accederá sólo el personal autorizado;
3. si el acceso se realiza con conexión a Internet se restringirá con un código de usuario y una contraseña (o cualquier otro medio que garantice la identificación y autenticación unívoca), que sólo serán conocidos por las personas autorizadas a acceder a dichas imágenes;
4. una vez instalado el sistema, se recomienda el cambio de la contraseña, evitando las fácilmente deducibles;

5. las imágenes serán conservadas durante un plazo máximo de 1 mes desde su captación;
6. las imágenes que se utilicen para denunciar delitos o infracciones se acompañarán a la denuncia y deberán 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;
7. y la petición de imágenes por las Fuerzas y Cuerpos de Seguridad se realizará en el marco de actuaciones judiciales o policiales. El requerimiento al titular del tratamiento será el documento que ampare a éste para ceder datos a las mismas o a los Juzgados y Tribunales que los requieran.

Existe cierta problemática en relación a la instalación de cámaras de videovigilancia, cuando estas se utilizan de forma disuasoria pero desconectadas, o en el caso de cámaras simuladas.[\[3\]](#)

En el primer caso, la instalación de cámaras de videovigilancia, incluso en los supuestos en los que no se encuentren en funcionamiento o conectadas, puede ser objeto de sanción igualmente si no cumplen con la normativa de protección de datos. La AEPD entiende que estas cámaras son reales y que pueden activarse sin esfuerzos excesivos en cualquier momento. Además, las personas que pasen frente a ellas no tienen forma de saber si están o no activadas, por lo que deben ser informadas de acuerdo con la normativa de cámaras de vigilancia.

Por lo tanto, aunque se tenga la cámara desconectada como medida disuasoria (incluido un local comercial o centro de trabajo), si queremos evitar sanciones por cámaras de seguridad desconectadas, deberemos cumplir con las obligaciones y requisitos recogidos en la normativa de protección de datos en cuanto a videovigilancia.

En el caso de cámaras “simuladas” colocadas como medida disuasoria (cámara falsa o sin ningún tipo de conexión), es poco probable que nos sancionen por colocarlas ya que, al no poder grabar, no hay ningún tratamiento de datos y, por tanto, no es de aplicación el RGPD. Sin embargo, se recomienda que la cámara “simulada” se oriente siempre hacia lugares permitidos, es decir, sobre espacios indispensables para el control laboral.

Servicio por tercero. Contrato de Encargado de Tratamiento

Si es una empresa externa quien presta los servicios consistentes en la instalación y/o mantenimiento de los equipos y sistemas de videovigilancia con acceso a las imágenes, siempre y cuando se cumpla con el deber de diligencia del considerando 81 del RGPD, será necesario celebrar un contrato entre el responsable del tratamiento y el encargado del tratamiento de acuerdo al artículo 28.3 del RGPD.

El contrato deberá contener la siguiente información: el objeto; la duración; la naturaleza y finalidad; el tipo de datos personales; categorías de interesados y las obligaciones y derechos del Responsable[\[4\]](#).

(Imagen: E&J)

Sanciones AEPD. Estadísticas

Las infracciones y sanciones previstas, por el uso indebido de las cámaras de videovigilancia son las siguientes:

- **Infracciones leves** (art. 74 LOPDGDD). Entra ellas se encuentran: (i) falta del cartel exigido de videovigilancia; (ii) no atender solicitud de derechos; (iii) registro de actividades de tratamiento (RAT) incompleto y (iv) falta del DPO (en los casos en que sea necesario su nombramiento). En estos casos, las sanciones serán de hasta 40.000 euros.
- **Infracciones graves** (art. 73 LOPDGDD). Entre ellas se encuentran: (i) obstaculizar los derechos de los interesados de forma reiterada; (ii) falta de medidas de seguridad en la conservación de las grabaciones; (iii) vulneración del principio de minimización de datos; (iv) falta de contrato de encargo de tratamiento si las cámaras las gestiona una empresa de seguridad externa; (v) no tener registro de actividades de tratamiento (RAT); (vi) falta de evaluación de impacto (EIPD) si es necesaria hacerla y (vii) falta de DPO si es necesario. En estos supuestos, las sanciones serán de 40.001 a 300.000 euros.
- **Infracciones muy graves** (art. 72 LOPDGDD). Entre ellas se encuentran: (i) usar las cámaras con otra finalidad diferente a la seguridad; (ii) grabar audio con las cámaras; (iii) no informar de las cámaras y su finalidad y (iv) vulnerar la confidencialidad de las grabaciones. En estos casos, las sanciones serán de 300.001 a 20 millones de euros (o el 4% de la facturación anual).

Es importante, por otra parte, resaltar la existencia de sanciones reguladas por la Ley de Seguridad Privada, que, en su art. 57.1.q, establece que: “El empleo o utilización, en servicios de seguridad privada, de medidas o de medios personales, materiales o técnicos de forma que se atente contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones, siempre que no constituyan delito”. Constituyendo una infracción muy grave, siendo sancionado con multa de 30.001 a 600.000 euros.

Así, a modo de ejemplo se citan las siguientes sanciones impuestas por la AEPD:

- Sanción a un establecimiento de 2.000 euros por colocar cámaras de seguridad orientadas al espacio público, incluso cuando estas cámaras, tal y como se alegó por el responsable del tratamiento, no estaban activadas. Infringiendo los principios de minimización de datos.
- Sanción a un restaurante de 1.500 euros por instalar cámaras de seguridad en la terraza, pero que además grababan una zona excesiva de la vía pública, en concreto el ancho de la acera y la calle paralela, captando imágenes de los transeúntes y vehículos que pasaban por la zona. (PS/00293/2020)
- Sanción a un local de recreativos de 6.000 euros por orientar sus cámaras de seguridad a la vía pública sin causa justificada, ya que las cámaras captaban imágenes de la vía colindante.
- Sanción de 1.000 euros [\[5\]](#), por colocación de cámaras y carecer de cartel de videovigilancia y registro de actividades de tratamiento, infracción del artículo 13.
- Sanción a establecimiento de 6.000 euros, por vulneración del principio de proporcionalidad previsto en

el artículo 4.1. y 4.2, dado que los monitores eran visibles por los propios clientes que accedían a local.

- Sanción a establecimiento[6] de 4.800 euros, por disponer de cámaras orientadas a la vía pública, infracción del principio de minimización de datos.
- Sanción de 1.000 euros[7], cámaras en el lugar de trabajo sin informar mediante el cartel informativo.

Desde el punto de vista estadístico, las sanciones por la instalación indebida de videocámaras o por incumplimiento de los requisitos para ello, han aumentado un 29% en el año 2023 con respecto al anterior. Con 2.197 expedientes en el año 2022 y 2.843 en el 2023, suponiendo un 13% de los expedientes tramitados por la AEPD en el año 2023.[8]

En relación con los procedimientos sancionadores y las multas, el área de actividad con mayor número de procedimientos resueltos en el año 2023 es la videovigilancia (164 procedimientos); aunque, el mayor volumen de multas corresponde a los casos relacionados con quiebras de datos personales. Esto se explica por la, generalmente, menor entidad de los casos de videovigilancia, tanto por su gravedad como por el tipo de responsable (personas físicas) y su relación con la eficacia de las multas (en términos de proporcionalidad y capacidad de disuasión), frente a la gran repercusión de las infracciones con la presencia de grandes compañías en el ámbito de las brechas de datos personales que afectan a gran número de clientes o ciudadanos. Son especialmente significativos los datos relativos a los titulares de ficheros de videovigilancia: tras los sectores de turismo y hostelería, el comercio y la sanidad, aparecen las comunidades de propietarios.

En conclusión, la observancia de todo lo anteriormente descrito, así como la actualización de la política de videovigilancia y la formación continua del personal son aspectos clave para garantizar el cumplimiento de la normativa de protección de datos en el ámbito laboral.

Fachada del edificio de la Agencia Española de Protección de Datos. (Imagen: AEPD)

Bibliografía

[1] Ficha práctica de videovigilancia-cámaras para el control laboral, publicada por la AEPD.

[2] Sentencia de la Audiencia Nacional (Contencioso), sec. 1ª, SAN 25-05-2023, rec. 574/2022; ROJ: SAN 2637:2023; ECLI: ES:AN:2023:2637.

[3] Guía sobre el uso de videocámaras para seguridad y otras finalidades de la AEPD. 6.3 Uso de cámaras simuladas.

[4] Guía sobre el uso de videocámaras para seguridad y otras finalidades de la AEPD. 2.3.8 Encargado de tratamiento: contratación de un tercero para el tratamiento de imágenes. / Art. 28.3 RGPD

[5] Expediente N°: EXP202105442 Resolución de procedimiento sancionador Agencia Española de Protección de Datos.

[6]

Procedimiento N°: PS/00135/2019 Resolución R/00275/2019 de terminación del procedimiento por pago voluntario.

[\[7\]](#) Procedimiento N°: PS/00506/2020 Resolución de procedimiento sancionador.

[\[8\]](#) Memoria Anual 2023 de la Agencia Española de Protección de Datos.