LA VIDEOVIGILANCIA LABORAL Y EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

A VIDEOVIXIANCIA LABORAL E O DEREITO A PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL

VIDEO SURVEILLANCE AND THE PRIVATE DATA PROTECTION RIGHT

IRIA NOYA RAMOS

Graduada en Derecho

Tutor:

MARCOS ANTONIO LÓPEZ SUÁREZ

Profesor Titular de Derecho Civil

31 de enero de 2020

ÍNDICE

ABREVIATURAS:

- **AEPD:** Agencia Española de Protección de Datos
- **CE:** Constitución Española
- **ECHR:** European Court of Homan Rights
- **ECLI:** Identificador Europeo de Jurisprudencia
- **ET:** Estatuto de los trabajadores
- **EIPD:** Evaluación de impacto en la protección de datos
- **CEDH:** Convención Europea de Derechos Humanos
- **LO:** Ley Orgánica
- **LOPDGDD:** Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales
- **RAE:** Real Academia Española
- **RGPD:** Reglamento General de la Protección de Datos
- **SAN:** Sentencia Audiencia Nacional
- **SSTC:** Sentencias del Tribunal Constitucional
- **STC:** Sentencia del Tribunal Constitucional
- **STEDH:** Sentencia del Tribunal Europeo de Derechos Humanos
- **STJUE:** Sentencia del Tribunal de Justicia de la Unión Europea
- **STS:** Sentencia del Tribunal Supremo
- **STSJ:** Sentencia del Tribunal Superior de Justicia
- **TC:** Tribunal Constitucional
- **TEDH:** Tribunal Europeo de Derechos Humanos

- **TOL:** Tirant Online
- **TS:** Tribunal Supremo
- **UE:** Unión Europea
- **Vid.:** Ver

I. INTRODUCCIÓN

La imagen de una persona en la medida que la identifique o la pueda identificar, constituye un dato de carácter personal y, por tanto, deberá ser protegida, ya que podría ser objeto de tratamiento ilícito.

Si partimos de la base de que la toma de imágenes de personas, por medios digitales, es un dato de carácter personal, son de aplicación las garantías respecto de los derechos inherentes a la persona, como el derecho a la intimidad, a la imagen, al honor o el derecho a la protección de datos implícito en el derecho a la limitación legal del uso de la informática (cfr. art. 18.4 de la Constitución española). Y ello, también en el ámbito laboral.

En el presente trabajo abordo el régimen de la videovigilancia en el ámbito laboral y los derechos fundamentales que puedan quedar afectados por esta práctica empresarial. Este trabajo se estructura en cuatro apartados principales, y en unas conclusiones finales, con arreglo al siguiente esquema:

En el primer apartado se estudia el concepto de videovigilancia. En este sentido se hace mención a los tipos de videovigilancia que nos podemos encontrar, y en concreto los utilizados en el ámbito laboral. Asimismo se hace una clasificación de los derechos fundamentales que se ven afectados por los sistemas de control empresarial, prestando especial atención al derecho a la intimidad, propia imagen y protección de datos.

A continuación se examinará el marco normativo de referencia existente para garantizar la no vulneración de los derechos fundamentales mencionados. A tal fin analizaremos las previsiones que al respecto se contienen 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, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

En el segundo apartado se realizará una exposición de los principios de tratamiento, considerados necesarios, para evitar la posible infracción de los derechos fundamentales de los trabajadores, afectados por los sistemas de videovigilancia del empresario. El análisis propuesto se completa con el estudio de las medidas de seguridad que la empresa ha de adoptar.

El apartado tercero tiene por objeto el examen de los distintos derechos que informan del tratamiento de datos de carácter personal. En particular, se puntualizará el derecho de transparencia e información, ya que este ha sido en los últimos años un tema que ha generado conflicto, en cuanto a su forma de interpretarse. Asimismo, se

expondrán, brevemente, el derecho de acceso, rectificación y supresión y otros derechos del interesado.

Y ya en el cuarto apartado, nos centraremos en el régimen sancionador, de forma que veamos qué sucede en caso de que el empleador deje de cumplir los requisitos establecidos para la utilización de los sistemas de videovigilancia laboral. Se analiza aquí los tipos de infracción, junto con las sanciones que se impondrán en el caso de incumplir los requisitos del uso de las videocámaras y vulnerar así los derechos fundamentales de los empleados.

Por último, se formulan las conclusiones correspondientes.

II. LA VIDEOVIGILANCIA

1. Videovigilancia y Derechos fundamentales

Puesto que el objeto de análisis es la videovigilancia es preciso concretar en qué consiste. Por tal, según el Diccionario de la Real Academia Española, cabría entender "*vigilancia a través de un sistema de cámaras, fijas o móviles"*[1].

A nivel legal, la videovigilancia es objeto de regulación en distintas normas[2]; sin embargo, en ninguna de ellas se define con precisión. Así, por tal motivo debemos acudir a la doctrina. En este sentido se ha pronunciado Calonge Crespo definiendo la videovigilancia como aquel proceso mecánico a través del cual se obtienen imágenes de personas y objetos, recogidos con una finalidad[3].

La videovigilancia generalmente tiene como finalidad salvaguardar la seguridad de los bienes y las personas. Asimismo en entornos empresariales se utiliza para verificar el cumplimiento por parte del trabajador de sus obligaciones y deberes laborales.

---

1 Definición dada por la RAE en el avance de la vigésimo tercera edición de la versión online de su diccionario de la Lengua Española, https://dle.rae.es/videovigilancia.

2 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, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

3 CALONGE CRESPO, I., "Videovigilancia y Seguridad Pública" en ETXBERRÍA GURIDI, J.F., *Videovigilancia: Ámbito de aplicación y derechos fundamentales afectados*, Ed. Tirant lo Blanch, 2010, p. 81.

La utilización de este medio tecnológico para la vigilancia incide de forma negativa sobre los derechos de las personas en tanto que capta y, en su caso, graba información en forma de imágenes. Por tal incidencia se fijan una serie de garantías[4].

Si aplicamos este concepto al ámbito laboral nos encontramos ante una estructura de captación de imágenes, e incluso sonido, en un espacio concreto, que pueden ser visualizadas, grabadas o reproducidas[5]. Por ello, la instalación de estos sistemas no debe ser algo arbitrario o casual, sino que debe responder a fines concretos y justificados.

No debemos olvidar la importancia de distinguir la videovigilancia utilizada por las Fuerzas y Cuerpos de Seguridad en lugares públicos[6], de la utilizada por un empresario en su centro de trabajo, dentro de un ámbito privado; y ello en su doble variante: ya sea cuando es el propio empresario es el que instala, graba y controla las grabaciones, ya sea cuando el encargado de realizar las grabaciones y de controlarlas es una empresa privada contratada por el empresario[7].

En muchos casos, el trabajador puede ver afectados los derechos fundamentales recogidos en la Constitución Española[8], por la utilización de la videovigilancia. Podríamos decir que los más vulnerados por los sistemas de videovigilancia serían, por un lado, el derecho a la intimidad personal o a su propia imagen, y por otro, la protección frente al tratamiento de datos de carácter personal[9].

---

4 Como lo son los principios de tratamiento y los derechos de los interesados.

5 ORDEÑANA GEZURAGA, I., "La Videovigilancia en el ámbito laboral. Especial incidencia en su utilización en el proceso laboral" en ETXBERRÍA GURIDI, J.F., *Videovigilancia: Ámbito de aplicación*… op.cit., pp. 46- 48.

6 La videovigilancia utilizada por las Fuerzas y Cuerpos de Seguridad en lugares públicos se regula mediante la Ley Orgánica 4/1997, de 4 de agosto, desarrollada y ejecutada mediante el Real decreto 596/1999, de 16 de abril. A estos efectos interesa saber que la instalación y uso de videocámaras o de cualquier otro medio análogo de captación, tratamiento y reproducción de imágenes por las Fuerzas y Cuerpos de Seguridad del Estado está sujeta a un régimen de autorización previa por órganos con participación judicial (cfr. art. 3 LO 4/1997). Asimismo, ha de referirse que la utilización de videocámaras debe sujetarse al principio de proporcionalidad, en su doble versión que es la idoneidad y la intervención mínima, que exige la consideración entre la finalidad pretendida y la posible afectación de los derechos fundamentales de los individuos (cfr. art. 6 LO 4/1997).

7 Se está haciendo referencia a la videovigilancia realizada a través de empresas de seguridad privada en el ámbito laboral, que ofrecen servicios de vigilancia y seguridad de personas y bienes, que tienen la consideración de actividades complementarias y subordinadas a la seguridad pública (art.1 Ley 5/2014, de 4 de abril, de Seguridad Privada).

8 Véanse recogidos en la CE la dignidad de la persona (art.10.1), la libertad ideológica (art.16), derecho a la intimidad personal o a su propia imagen (art.18.1) y la protección frente al tratamiento de datos de carácter personal (art.18.4).

9 ORDEÑANA GEZURAGA, I., "La Videovigilancia en el ámbito laboral...", op. cit., pp. 46- 47.

El primero de ellos implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás y, en consecuencia, garantizar, como declara el TC en su sentencia 70/2009, del 22 de abril "el secreto sobre la vida personal, prohibiendo a los terceros, particulares o poderes públicos, decidir sobre los contornos de la vida privada"[10], protegiendo así su intimidad individual e imponiendo el deber de abstenerse a todo tercero de acceder a la esfera íntima.

En conexión con lo expuesto, cabe añadir que el artículo 18.1 del 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, si bien garantiza la inviolabilidad de la vida personal, admite una excepción, indicando que *"Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible"*.

El derecho a la propia imagen trata de salvaguardar un ámbito propio, pero no íntimo, y proporciona una protección frente a las reproducciones de la imagen propia que afecta a esa esfera personal, "reconociendo a la persona la facultad de evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de toda persona"[11].

No podemos negar que la videovigilancia, además de afectar a la intimidad y a la imagen del trabajador, perjudica también al derecho fundamental de la protección de datos el cual es inherente a todos los ciudadanos[12].

El derecho a la protección de datos personales se encuentra garantizado, asimismo, en el ámbito del Consejo de Europa, por el artículo 8 del Convenio de Roma de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales consagra el derecho al respeto a la vida privada y familiar[13].

---

10 Vid. STC 70/2009, de 22 de abril (ECLI:ES:TC:2009:70).

11 Vid. STC 81/2001, de 26 de marzo (ECLI:ES:TC:2001:81).

12 Véase artículo 18.4 CE: "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."* Asimismo, el marco legislativo europeo también reconoce este derecho a la protección de datos y obliga a todos los Estados miembros a garantizarlo a sus ciudadanos.

13 El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea en sus apartados 1 y 2 establece: *"Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación".*

Para nuestro Tribunal Constitucional, el artículo 18.4 de la Constitución consagra un derecho fundamental autónomo y diferente del derecho a la intimidad, "una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de las personas (...) un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática"[14].

Posteriormente, en la sentencia 292/2000, de 30 de noviembre, estableció que el derecho a la intimidad tiene la función de proteger frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar, mientras que "el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado" [15].

De este modo la protección de datos personales no se reducirá exclusivamente a la protección de los datos íntimos de la persona, sino que comprenderá "cualquier tipo de dato personal, sea íntimo o no, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal" [16].

Este derecho tiene como función garantizar un control a una persona sobre sus datos personales, sobre su uso y destino, con la finalidad de impedir un tráfico ilícito y lesivo para la dignidad y otros derechos del afectado; de ahí, que se extienda a cualquier tipo de dato personal, cuya utilización por terceros puede afectar a los derechos fundamentales. Y sea necesario un previo consentimiento para su recogida y uso de los datos personales[17].

Para evitar el posible exceso que vulnere los derechos fundamentales por la instalación de cámaras de videovigilancia, debemos acudir a la regulación, a pesar de que esta no sea específica, y a las resoluciones de los distintos Tribunales que se han pronunciado sobre la problemática, como veremos más adelante.

---

14 Vid STC 254/1993, de 20 de julio (ECLI:ES:TC:1993:254).

15 Vid. STC 292/2000, de 30 de noviembre (ECLI:ES:TC:2000:292).

16 Vid. STC 292/2000, de 30 de noviembre (ECLI:ES:TC:2000:292).

17 Vid. STC 292/2000, de 30 de noviembre (ECLI:ES:TC:2000:292). En ella se declara que el derecho de protección de datos "también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos".

2. Marco normativo de referencia

Como consecuencia del proceso de simplificación de contenido del derecho que afecta al trabajador, se ha llegado a excluir del ámbito protegido el derecho a la dignidad e intimidad del trabajador en las relaciones profesionales, de forma que se ha permitido cualquier dispositivo de control laboral del trabajador[18].

La utilización de la videovigilancia en el ámbito laboral pese a hallarse regulada, lo cierto es que el progreso de la técnica evoluciona más rápido que la norma; por ello, surge la necesidad constante de adaptación. Y se hace evidente el papel de los Tribunales, en orden a la resolución de las controversias, mientras no se concreta ese ajuste, y el carácter cambiante de sus pronunciamientos.

Así, a título de ejemplo, los Tribunales venían admitiendo que los empleadores, sin demasiadas contemplaciones, utilizaran mecanismos que permitieran la captación de imágenes para comprobar el cumplimiento por parte del trabajador de sus obligaciones laborales, de manera que se asumía que el centro de trabajo era un lugar público en el que el derecho a la intimidad no se veía afectado. Sin embargo, el TC desautoriza la permisividad de dichos sistemas de grabación, produciéndose un punto de inflexión, con respecto a los límites de la videovigilancia en el ámbito laboral[19].

Como decíamos, estas cuestiones, sin perjuicio de que existan eventuales lagunas, se encuentran reguladas por el legislador a través de diversas normas. En primer lugar, debe hacerse referencia a los sistemas de videovigilancia de las Fuerzas y Cuerpos de Seguridad[20] y control en los centros penitenciarios y al control, regulación, vigilancia y disciplina del tráfico[21].

Fuera de los supuestos indicados, el tratamiento de datos se regirá por su legislación específica; por ello será necesario abordar el ámbito privado de la videovigilancia, donde además de tener en cuenta el ET, no podemos olvidarnos de la aplicación de la normativa de protección de datos.

---

18 GOÑI SEIN, J. L., *"La Videovigilancia empresarial y la Protección de datos Personales",* Thomson-Aranzadi, Pamplona, 2007, p. 28-29.

19 Vid. STC 98/2000, de 10 de abril (ECLI:ES:TC:2000:98) y STC 186/2000, de 10 de julio (ECLI:ES:TC:2000:186).

20 Ley Orgánica 4/1997, de 4 de agosto de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

21 Se regirá por la legislación de transposición de la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo de 27 de abril de 2016, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

Desde el contexto de la libertad de empresa[22], el artículo 20 del ET regula el poder de dirección y control de la actividad laboral por parte del empresario, y establece los parámetros por los que se orienta dicho poder, diligencia y buena fe, que no solo ha de ser cumplido por el empresario sino también por el trabajador.

En cuanto a la concreción del poder de control, la norma estatutaria se limita a indicar que *"el empresario podrá adoptar las medidas que estime más oportunas",* con el fin de *"verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales",* con un límite, la *"consideración debida a su dignidad".*

De esta forma, concurren varios intereses que confluyen con el bien jurídico protegido de la intimidad del trabajador y el derecho del empresario a controlar la actividad laboral. Este último se vale de medidas, como la videovigilancia.

La intimidad de los trabajadores se ve amenazada por las herramientas digitales, que permiten las funciones de control otorgadas por el Estatuto de los Trabajadores al empleador, ya que este podrá velar por sus legítimos intereses, controlando el grado de cumplimiento de las tareas encomendadas a los trabajadores.

Surge así la problemática de conflicto entre el derecho al control laboral y los derechos más esenciales de los trabajadores[23], en particular, respecto a su derecho a la intimidad y a la protección de datos que el propio ET reconoce en su artículo 4.2.e., a cuyo tenor, los trabajadores tienen derecho: *"Al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo".*

Resulta relevante refiere al nuevo contenido del artículo 20 bis del ET que regula el derecho a la intimidad de los trabajadores en relación con el entorno digital y a la desconexión[24].

> "*Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la*

[22] Véase artículo 38 CE: "*Se reconoce la libertad de empresa en el marco de la economía de mercado. Los poderes públicos garantizan y protegen su ejercicio y la defensa de la productividad, de acuerdo con las exigencias de la economía general y, en su caso, de la planificación.*"

[23] SÁNCHEZ-RODAS NAVARRO, C., "Videocámaras y poder de vigilancia", *Aranzadi Social*, núm.5, Tomo IX, 1999, p.1127*:* "Quiere con ello decirse que intramuros de la empresa y en horario laboral apenas existe espacio de intimidad que salvaguardar por cuanto que en tales circunstancias la obligación del trabajador es cumplir con su prestación laboral...".

[24] Las Disposiciones Finales que incorpora la LOPDGDD. La Disposición final decimotercera modifica el Texto Refundido de la Ley del Estatuto de los Trabajadores.

legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

Por ello, la utilización de dispositivos de videovigilancia requiere de reglas y limitaciones que modulen la facultad de control empresarial para adecuarla a los usos y convenciones que amparan unas expectativas básicas de la intimidad de los trabajadores y que no conviertan ese uso en una intromisión ilegítima.

En el ámbito de la protección de datos, debemos hacer mención en primer lugar al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de datos, cuyo objetivo es proteger el tratamiento de los datos personales de los ciudadanos y propiciar que cada persona tenga control sobre el uso de sus datos personales.

Cabe decir que el RGPD no contiene previsión alguna en cuanto al uso de las imágenes con finalidades de seguridad como dato personal. Salvo lo dispuesto en su artículo 88 sobre las normas específicas que cada Estado miembro puede desarrollar, garantizando la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral:

> *"dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo."*

En segundo lugar, cabe referirse a la LOPDGDD, que introduce, por primera vez, en su artículo 22, la regulación de la gestión de los datos personales obtenidos mediante videovigilancia y los plazos máximos de almacenamiento de estas imágenes y de puesta a disposición de las mismas ante la autoridad competente. Por su parte los artículos 89 y 90 del mismo cuerpo legal establecen una referencia específica al ámbito laboral[25]; reconocen la facultad de los empleadores para tratar imágenes o datos obtenidos a través de sistemas de cámaras, videocámaras y de geolocalización para el ejercicio de las funciones de control de los trabajadores.

A la vez, los referidos preceptos imponen a los empleadores la obligación de *"informar con carácter previo, de forma expresa, clara y concisa, a los trabajadores"*.

[25] Hasta la fecha, como se observaba al principio del trabajo, la ausencia de una regulación específica del derecho a la protección de datos de carácter personal en el ámbito laboral había sido colmada mediante las doctrinas jurisprudenciales del Tribunal Constitucional y del Tribunal Supremo, que habían generado un cuerpo consolidado de criterios interpretativos y aplicativos en esta materia, no exento de fricciones con la doctrina emanada del Tribunal Europeo de Derechos Humanos.

Esta información a los trabajadores se convierte en una exigencia inicial para poder legitimar la intervención empresarial, convirtiéndose en un punto fundamental en el sistema de garantías de los trabajadores frente al control empresarial.

Además, la videovigilancia se encuentra sometida a limitaciones cuando se identifican singulares riesgos para la privacidad de los trabajadores. Así se establece en su artículo 89.2 LOPDGDD:

> *"En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos".*

Y lo mismo sucede cuando los dispositivos de grabación de sonidos son invasivos en la intimidad de los trabajadores, y no se adecua a las limitaciones del principio de intervención mínima y plazos específicos para la supresión. Así, se recoge en el apartado tercero del artículo 89.3 LOPDGDD:

> *"La utilización de sistemas para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los 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 el principio de proporcionalidad, el de intervención mínima y las garantías previstas".*

Estas previsiones legales constituyen un marco mínimo de protección de los trabajadores que podrá ser ampliado en el marco de la negociación colectiva[26], pudiendo establecer garantías adicionales de los derechos y libertades relacionadas con el tratamiento de los datos personales de los trabajadores y salvaguardar los derechos digitales en el ámbito laboral.

III. LOS PRINCIPIOS DEL TRATAMIENTO

La captación de imágenes deberá responder exclusivamente a la finalidad de preservar la seguridad de las personas y bienes, debiendo estar siempre sujeta la instalación de estos elementos de grabación a los criterios de proporcionalidad y necesidad, y sin que, en ningún caso, se pueda hacer uso de las imágenes para fines diferentes de aquellos para los que fue autorizada su instalación.

[26] RALLO LOMBARTE, A., "Del derecho a la protección de datos a la garantía de nuevos derechos digitales", en *Tratado de protección de datos,* 2019, Tirant Online (TOL7218.393).

De este modo, no cabe captar imágenes para el control directo ni indiscriminado de los trabajadores ni tampoco la instalación de sistemas audiovisuales de control en los lugares de descanso o esparcimiento, tales como vestuarios, aseos, comedores y análogos.

El hecho de que la norma establezca la obligación de los empleadores de informar, con carácter previo, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida, no la hace menos cuestionable y sujeta a la necesaria crítica. Y es que en muchas ocasiones la vigilancia responde al fin de justificar un despido y no a la necesidad de control general.

Debido a esto, la legislación sobre protección de datos personales intenta conjurar los riesgos que para los derechos de las personas suponen el tratamiento de sus datos personales y al mismo tiempo garantizar los intereses, a través de una serie de límites y requisitos.

El RGPD integra ambos tipos de garantías bajo la denominación de principios relativos al tratamiento y los derechos de las personas en sus Capítulos II y III, respectivamente.

El artículo 5 del RGPD regula los principios básicos que deberán respetarse en la recogida, tratamiento, uso y almacenamiento de los datos personales - principios que reproduce, en gran medida, la LO 3/2018 - y que son: el principio de licitud, limitación de la finalidad, minimización, exactitud, conservación de los datos y de integridad y confidencialidad; asimismo también se deben tener en cuentas la medidas responsabilidad proactiva.

Estos principios no sólo se limitan a informar de toda la normativa de protección de datos personales, sino que, además, se configuran como elementos fundamentales a tener en cuenta en aplicación práctica, por lo que será necesario su cumplimiento en cada supuesto concreto de tratamiento, garantizando una utilización racional y razonable de los datos personales[27].

1. Principio de licitud en el tratamiento

El principio de licitud se encuentra regulado en el apartado a. del artículo 5 del RGPD, de acuerdo con el cual los datos personales serán tratados *"de manera lícita, leal y transparente en relación con el interesado"*; dicha previsión ha de completarse con lo dispuesto en el apartado 1º del artículo 6 del RGPD.

[27] PUENTE ESCOBAR, A., 8. ª Sesión Anual Abierta de la AEPD. Gran Auditorio Ramón y Cajal. 29 de junio de 2016.

Se trata de un concepto jurídico indeterminado que implica el cumplimiento de las prescripciones normativas en el tratamiento de datos, tales como la veracidad de los datos, legitimidad de los fines del tratamiento, la adopción de las medidas de seguridad, el cumplimiento de los deberes de conservación, información, u obtención de consentimiento, entre otros.

Los datos personales deberán recogerse sin engaños o falsedades por parte de quien los solicita, prohibiéndose la utilización de medios fraudulentos, desleales o ilícitos. En otros términos, de este principio deriva "la necesidad de que los datos personales que se recojan en cualquier fichero sean obtenidos por medios lícitos, y de esta forma sea conocida su utilización por los afectados, siendo los responsables de su obtención quienes responden del cumplimiento de esta obligación"[28].

La propia norma regula las condiciones que debe reunir un tratamiento de datos para que pueda ser considerado lícito y la incidencia que la finalidad del tratamiento tiene sobre la licitud.

El artículo 6 RGPD estipula que el tratamiento solo será lícito si se cumple al menos una de las condiciones, que se desglosan en los apartados a) hasta f):

En el apartado a. se establece la licitud del tratamiento cuando *"el interesado dio su consentimiento para el tratamiento de sus datos (...) para uno o varios fines específicos…"*

Como recoge el RGPD en su artículo 4, "*el consentimiento es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*".

En el ámbito laboral, sería la casilla a marcar en el contrato laboral, donde se consiente el uso de la imagen propia, para la publicidad y otra casilla para grabación en el horario de trabajo.

Recordemos que el consentimiento se da para una finalidad concreta y que en el caso de que exista una pluralidad de fines será preciso que consten de manera específica para que el consentimiento que damos se otorgue para todas esas finalidades[29].

---

[28] SAN 4202/2011, de 22 septiembre (ECLI:AN:2011:4202).

[29] VALDECANTOS, M., "El consentimiento como base legitimadora del tratamiento en el Reglamento Europeo de protección de datos", *Actualidad Civil* núm. 5, mayo de 2018.

Cabe añadir que, aunque se disponga del consentimiento inicial, el interesado tendrá derecho a retirar el mismo en cualquier momento, lo que no afectará a la licitud. Igualmente el RGPD establece que los interesados deben tener derecho a acceder a los datos personales recogidos con el fin de conocer y verificar la licitud del tratamiento.

En el apartado b se estipula que *"el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales…"*

El tratamiento de datos basado en la ejecución de un contrato viene dado por la necesidad y legitimidad del uso de datos relativos al cumplimiento de la finalidad objeto del contrato que une a ambas partes. Así la realización de las nóminas de los trabajadores viene legitimada por la ejecución del contrato laboral que une a ambas partes.

En el apartado c. se estipula que *"el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento…"*

Así acontece, por ejemplo, con la obligación de conservación de los datos contenidos en los contratos laborales durante 5 años por imperativo de la Ley sobre Infracciones y Sanciones en el Orden Social.

En el apartado d. se estipula que *"el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física…"*

En el día a día más cercano, dicha legitimidad la encontraríamos en aquellos supuestos en que un médico tenga que tratarnos en urgencias y pueda acceder a nuestros datos e historial clínico por un interés vital, ya que si el interesado está inconsciente el médico no dejará de tratarlo con base en la protección de los intereses vitales. En el caso laboral podríamos hacer mención a la situación en la que se produce un accidente y hay que actuar de emergencia, ya que la vida del trabajador puede estar en peligro.

Y en el apartado f. se estipula que *"el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño."*

La existencia de un interés legítimo requiere una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin.

Queda así vinculado el principio de licitud al principio de transparencia, e igualmente vinculado con la información, debido que la misma debe facilitarse de forma comprensible y accesible. Por tanto, el tratamiento no será leal y lícito si la información no está accesible o no es comprensible. Así se colige del Considerando 39, a cuyo tenor:

> *"toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento".*

En la LOPDGDD no se hace una mención expresa en su articulado al citado principio, si bien en el preámbulo se especifica que en el Título IV se recogen "*Disposiciones aplicables a tratamientos concretos*", incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de todos los tratamientos lícitos[30].

2. Principio de limitación de la finalidad

El principio de limitación de la finalidad recogido en el apartado b. del artículo 5 del RGPD determina que el propósito del tratamiento debe ser clara y estar determinada con anterioridad a que los datos sean recogidos y tratados por el responsable. De esta, el afectado por los sistemas de videovigilancia, cuyos datos son objeto de tratamiento, debe conocer la finalidad de dicho tratamiento. Por ello, el contenido de la información facilitada al interesado se configura como un elemento esencial. Según esto, los datos sólo podrán recogerse y tratarse de acuerdo con una finalidad legítima y determinada y no podrán recogerse para finalidades contrarias a las leyes o al orden público[31].

Este principio no sólo protege la privacidad de la persona, sino que deja que los responsables del tratamiento innoven a la hora de encontrar la mejor solución de protección. De esta manera se transforma en un instrumento de protección cautelar que

---

[30] PUENTE ESCOBAR, A., "Principios y licitud del tratamiento", en *Tratado de protección de datos*, op.cit. (TOL7218.395).

[31] Conforme a los artículos 13 y 14 del RGPD.

obliga al responsable del tratamiento a identificar los riesgos específicos derivados de su tratamiento contra los derechos fundamentales del interesado. Podríamos decir que su objeto es controlar el riesgo causado por el tratamiento de datos que se produjo en una fase posterior y se añade a los riesgos que se identificaron previamente[32].

El RGPD dispone que los datos no podrán ser tratados para fines incompatibles con los que justificaron su recogida. No cabe duda de que cualquier tratamiento deberá contar con una base jurídica adecuada, ya que, si no, se estaría vulnerando lo dispuesto en el artículo 6.1 del RGPD; por ello, deberá atenderse a los criterios del mismo para la determinación de la no incompatibilidad de la finalidad que justifica el tratamiento ulterior, lo que exigirá llevar a cabo una evaluación de dicho grado de no incompatibilidad para cada supuesto concreto[33].

El cumplimiento de este requisito impide que una vez que los datos hayan sido utilizados para la finalidad legal, puedan ser reutilizados para el cumplimiento de objetivos distintos a aquellos que motivó su solicitud. Se relaciona así este principio con el derecho de supresión del artículo 17 de RGPD que establece que el interesado tendrá el derecho y el responsable del tratamiento el correlativo deber de suprimir los datos cuando *"ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo".*

3. Principio de minimización

El principio de minimización regulado en el apartado c. del artículo 5 del RGPD pretende limitar el uso de datos estrictamente a aquellos que sean considerados como adecuados. Los datos que sean objeto de tratamiento a través de la videovigilancia han de ser tratados únicamente para la finalidad concreta prevista, como ya indicamos anteriormente, de manera que los datos personales sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Así las cosas, el principio de minimización está estrechamente ligado al principio de proporcionalidad[34]. En cuanto a la extensión de este último, el TC ha tenido ocasión de

---

[32] GRAFENSTEIN, M.V., *The Principle of Purpose Limitation in Data Protection Laws*, Nomos, 2018, p. 109 y ss.

[33] Véase el artículo 5.1 b) del RGPD*, "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)".*

[34] En este sentido, debemos de tener en cuenta el límite de la calidad de los datos, entendida desde dos perspectivas: que la información solicitada a los titulares de los datos no se exceda de los fines para los que es recabada; y la obligación del responsable del fichero a mantener las listas actualizadas para que reflejen la situación actual del titular de los datos. Por tanto, la recopilación de imágenes debe respetar el

pronunciarse declarando lo siguiente: "la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta con recordar que para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes:

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)."[35]

El principio de proporcionalidad no solo se limita el tratamiento de datos en el sentido de adecuarlo a unos fines específicos sino que además impone la necesidad de adoptar las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales[36]. Así cobra valor el concepto de necesidad de manera que, si el objetivo se lograse sin realizar un tratamiento de datos, los mismos no deberían ser tratados. Además, dicha limitación a lo necesario debe ser evaluada desde un punto de vista tanto cuantitativo como cualitativo[37].

El RGPD indica que el derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad, por lo que exige que los mismos se limiten a lo necesario para el

---

principio de calidad de los datos, y no todos los datos que superen los requisitos para su captación serán válidos, pues si éstos son abusivos podrán también vulnerar dos los derechos de los empleados.

35 Vid. STC 186/2000, de 10 de julio (ECLI:ES:TC:2000:186).

36 Como toda medida susceptible de atentar contra derechos fundamentales, el sistema de videovigilancia debe superar el juicio clásico de constitucionalidad:
a) Juicio de idoneidad: debe ponderarse si la captación de imágenes es un medio idóneo para conseguir el objetivo propuesto; imaginemos a un empleado frente a un ordenador cuya imagen no alcance a adivinar la actividad en el monitor: no sería adecuada puesto que captar la imagen del empleado no revelaría su actividad laboral.
b) Juicio de necesidad: debe ponderarse si la videovigilancia es el medio menos intrusivo, pues debe tener un carácter subsidiario, como toda medida restrictiva de derechos. Por ello, debe justificarse su necesidad en relación con medios igual de eficaces para el mismo fin.
c) Juicio de proporcionalidad en sentido estricto: debe atender a un equilibrio entre los perjuicios causados (intromisión) y los beneficios que suponga su uso (control laboral, patrimonio empresarial, etc.).

37 Así se establece en el artículo 39 RGPD: *"Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios."*

cumplimiento de dicha finalidad. Así, el tratamiento de datos personales para lograr una finalidad específica no puede ser excesivo, sino que los datos con base en la proporcionalidad deben ser tratados de manera idónea al fin que se quiere conseguir[38].

Por ello, el uso de videocámaras debe basarse en la idoneidad y en la intervención mínima, la cual requiere el equilibrio entre la finalidad perseguida y el posible daño al derecho al honor, a la propia imagen y a la intimidad de las personas.

La LOPDGDD, en dos preceptos, remarca la necesidad de este principio. Así sucede en el artículo 69.1 en cuanto a las medidas provisionales y de garantía de derechos en los procedimiento en caso de posible vulneración de la normativa[39], y también, como se ha indicado, en el artículo 89.3 en cuanto al derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

Por todo ello, el principio de minimización de datos, no es otra cosa que restringir la recogida de datos a los que sean estrictamente adecuados, pertinentes y limitados en relación con los fines para los que son tratados, como el caso referido en el artículo 89.2. LOPDGDD, relativo a los lugares de descanso de los trabajadores.

4. Principio de exactitud

El principio de exactitud regulado en el apartado d. del artículo 5 del RGPD, obliga al responsable del tratamiento a actuar con la diligencia necesaria para hacer un buen uso de los datos, en el sentido de que estos sean correctos, completos y actuales[40].

De este modo, la garantía de la exactitud de los datos por parte del responsable del tratamiento no sólo implica la obligación de atender a las solicitudes de rectificación o supresión de los datos inexactos, incompletos, inadecuados o excesivos, sino que conlleva también una obligación activa por parte de aquél, que deberá garantizar la

[38] PUENTE ESCOBAR, A., "Principios y licitud del tratamiento", en *Tratado de protección de datos*, op.cit. (TOL7218.395).

[39] De conformidad con lo dispuesto en el artículo 69.1 LOPDGDD "*Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado*".

[40] Según este principio corresponde al responsable del tratamiento asegurarse de la exactitud de los datos, es decir, que responden a la situación real del interesado. Vid. STS 545/2013, de 29 de enero (ECLI:ES:TS:2013:545).

rectificación o supresión de los datos que se encuentren en cualquiera de esos supuestos[41].

En este mismo sentido, el artículo 39 del RGPD indica que *"todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos*". La obligación del responsable de corregir aquellos datos que sean inexactos es correlativo al derecho de rectificación de los interesados, expresamente reconocido en el artículo 16 del Reglamento.

En la LOPDGDD en su artículo 4, se articula el principio de exactitud de los datos, en el que, además de remitir al citado precepto del RGPD, se indica que "*(...) no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos (...)".*

Debemos tener en cuenta que este principio está enlazado con el derecho a la limitación del tratamiento regulado en el artículo 18 del RGPD y en el artículo 16 de la LOPDGDD.

5. Conservación de los datos

El principio de conservación de los datos, regulado en el apartado e. del artículo 5 del RGPD, establece que los datos personales serán mantenidos, de forma que se permita la identificación del afectado, solo durante el tiempo necesario para los fines del tratamiento de esos datos.

Este principio está directamente relacionado con el principio de limitación de la finalidad y el derecho a la supresión de los datos cuando hayan dejado de ser precisos para la finalidad legítima que justificó su recogida y tratamiento. El artículo 13.2. RGPD establece que el responsable de tratamiento deberá informar del plazo previsto durante el cual se conservarán los datos personales o *"cuando no sea posible, los criterios utilizados para determinar este plazo."*

Desde la fecha en que resulta de aplicación el RGPD, se ha desplazado la mayor parte 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 videocámaras; sin embargo, lo dispuesto en su artículo 6 puede considerarse que sigue en vigor. En concreto en el referido precepto se regula el

[41] PUENTE ESCOBAR, A., "Principios y licitud del tratamiento", en *Tratado de protección de datos*, op.cit. (TOL7218.395).

plazo de conservación de las imágenes captadas por los sistemas de videovigilancia y se establece que se proceda a la supresión en el plazo máximo de un mes, salvo en aquellos supuestos que se deban conservar para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

En consecuencia con lo expuesto, la LOPDGDD añade como excepción al plazo máximo de conservación de un mes que, en caso de ser necesario acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones, el plazo se prorrogará. En tal caso, *"las imágenes deberán ser como dispone el artículo 22.3 LOPDGDD, puestas a disposición de la autoridad competente en el plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación".*

6. El principio de integridad y confidencialidad

El principio de integridad y confidencialidad se encuentra regulado en el apartado f. del artículo 5 del RGPD de acuerdo con el cual los datos personales serán "*tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas*."

La voluntad del legislador con la redacción de este precepto no puede ser otra que la de establecer con carácter general un deber de confidencialidad y secreto por parte de quien trata datos personales, siendo necesario que este deber persista incluso con el cese en el tratamiento de los datos[42].

Podríamos decir que, en consecuencia, los derechos de los afectados quedarían garantizados en tanto persista el tratamiento de sus datos, cediendo, a falta de previsión legal en contrario, en el momento que cese dicho tratamiento.

Por medio de este principio se pretende garantizar los derechos de los afectados, ante la constante evolución de las nuevas capacidades de proceso de los ordenadores, en la microelectrónica y en el software, el desarrollo de Internet y de la computación en la nube, lo que ha permitido la proliferación de sistemas informáticos potentes y fáciles de utilizar, con el consiguiente incremento de "los riesgos que amenazan a los datos

[42] PUENTE ESCOBAR, A., "Principios y licitud del tratamiento", en *Tratado de protección de datos*, op.cit. (TOL7218.395).

almacenados y procesados por ellos y, en consecuencia, a los ciudadanos a quienes dichos datos conciernen"[43].

La seguridad constituye uno de los aspectos que forman parte del contenido del derecho fundamental y "se convierte en un elemento esencial en la protección de las personas a través de la protección de sus datos y de los tratamientos de que forman parte"[44]. Esta protección deberá abarcar tanto la confidencialidad de la información como la disponibilidad e integridad de la misma[45] .

Por último, este principio exigirá un deber general de confidencialidad sobre la información personal por parte del responsable y el encargado del tratamiento y de todas aquellas personas que intervengan en alguna fase del mismo. Y se debe tener en cuenta que esta obligción deberá subsistir después de que haya finalizado la relación con el responsable del tratamiento[46].

7. Medidas de responsabilidad proactiva de seguridad de los datos, evaluación de impacto y códigos de conducta

Los datos personales obtenidos con las videocámaras serán tratados de manera que se garantice su adecuada seguridad. Esto incluye la protección contra el uso no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

En primer lugar nos centraremos en las medidas de responsabilidad proactiva, como principio esencial en el tratamiento de datos personales. En concreto, el artículo 5 del RGPD, en su apartado 2, señala que el responsable del tratamiento debe estar en condiciones de demostrar y proporcionar evidencias del cumplimiento de los principios enumerados en dicho precepto.

El RGPD establece un catálogo de medidas que el responsable y, en ocasiones los encargados, deben aplicar para garantizar que los tratamientos sean conformes a la

---

43 CUEVA CALABIA, J. L.: "La LORTAD y la seguridad de los sistemas automatizados de datos personales", *Actualidad Informática Aranzadi*, número 13, octubre, 1994, p. 7.

44 REBOLLO DELGADO, L., SERRANO PEREZ, M. M.: *Introducción a la protección de datos*, Dykinson, Madrid, 2008, p. 139.

45 DEL PESO NAVARRO, E., RAMOS GONZALEZ, M.A., DEL PESO RUIZ, M., y DEL PESO RUIZ, M.: *Nuevo Reglamento de protección de datos de carácter personal: Medidas de seguridad*, Ediciones Díaz de Santos, 2012, p. 309 y ss.

46 Véase artículo 5 de la Ley Orgánica 3/2018.

norma europea. No obstante, es preciso matizar que, no en todos los casos, estas medidas deben aplicarse obligatoriamente[47].

También debe hacerse mención al análisis de riesgos y medidas de seguridad. El RGPD obliga a que los responsables lleven a cabo una valoración del riesgo de los tratamientos que realicen, con el fin de establecer las medidas a aplicar. Y es que el RGPD no establece medidas de seguridad estáticas sino que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales[48].

Así, según el artículo 32 del RGPD, las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se definen en función del estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

En definitiva el primer paso para determinar las medidas de seguridad será la evaluación del riesgo del tratamiento de las imágenes en el ámbito laboral y, una vez evaluado, será necesario determinar las medidas de seguridad dirigidas a la reducción y eliminación de tales riesgos para el tratamiento de los datos.

Otro de los conceptos que se debe tener en cuenta es la evaluación de impacto en la protección de datos (EIPD). Se trata de una herramienta de carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

En este orden de ideas, cabe también a aludir a los Códigos de conducta, que son un conjunto de normas que voluntariamente asume la empresa con el objetivo de facilitar el cumplimiento de una determinada normativa o lograr un comportamiento ético. En el caso de la videovigilancia en el ámbito laboral, se adoptarían los Códigos de conducta para evitar la posible vulneración de los derechos fundamentales de los empleados.

---

47 El RGPD condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados. En algunos casos, prevé que determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos). Y en otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve (por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad).

48 SAIZ PEÑA, C., A., "Seguridad de los datos, evaluación de impacto, códigos de conducta y certificaciones", en *Tratado de protección de datos.*, Tirant Online, 2019 (TOL7218.403).

Estos Códigos también son considerados una medida proactiva y se encuentran regulados en el RGPD, para que las organizaciones puedan adherirse a ellos. Con el objetivo de potenciar que sean los propios responsables quienes faciliten la aplicación efectiva de la normativa, teniendo en cuenta las características específicas de su sector de actividad y las necesidades de las empresas participantes[49].

IV. DERECHOS DE LOS INTERESADOS

EL RGPD regula en el Capítulo III (arts. 15 a 20) [50] los derechos del interesado en materia de protección de datos. El ejercicio de los derechos seguirá siendo una herramienta para asegurar la garantía sobre el uso de los datos personales, pero también supondrá un reto para las empresas, que tendrán que establecer límites y plazos para el tratamiento de esos datos.

1. Deber de información y transparencia

El deber de información y el de transparencia se encuentran regulados en el RGPD y conllevan la obligación de informar al interesado de la finalidad de la obtención de los datos; en concreto, el artículo 5 del RGPD incluye, dentro de los principios relativos al tratamiento, el principio de transparencia, estableciendo que los datos personales serán *"tratados de manera lícita, leal y transparente en relación con el interesado"*.

El objetivo de este principio debe ser garantizar que el interesado, de un modo efectivo que, *"sea consciente de la lógica a que obedece el tratamiento de sus datos personales"* para que de verdad pueda tener un auténtico poder de disposición sobre ellos.

Por ello, junto con la observancia de los principios mencionados, sabemos que para considerar válida la captación de imágenes, uno de los requisitos principales en la práctica es la información de la implantación y finalidad del sistema de videovigilancia.

En virtud de este principio y de acuerdo con lo establecido en el artículo 12 RGPD, el responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, cualquier comunicación

---

49 SAIZ PEÑA, C., A., "Seguridad de los datos, evaluación de impacto, códigos de conducta y certificaciones", en *Tratado de protección de datos.*, op.cit. (TOL7218.403).

50 Estos también se encuentran descritos en los Considerando 58 a 71del RGPD.

con arreglo a los derechos recogidos en el capítulo III del RGPD, así como el supuesto de que se produzca una violación de datos de acuerdo con lo previsto en el artículo 34.

Debemos tener en cuenta que una información genérica no será suficiente, sino que deberá indicarse necesariamente el tratamiento de los datos y finalidad a que se destinan los datos personales, junto con la base jurídica del tratamiento.

Esta información debe ser clara, concisa, transparente, de fácil acceso. En estos términos, los requisitos informativos no pueden ni deben limitarse a la colocación de cartelería. La información, según lo establecido en el artículo 12 del RGPD, será facilitada por escrito o por otros medios, incluidos los electrónicos como, por ejemplo, un sitio web. También podrá facilitarse verbalmente cuando lo solicite el interesado y siempre que se demuestre la identidad del interesado por otros medios. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse, asimismo, a través de iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto[51].

En cuanto al distintivo informativo, al que hacíamos mención, se encuentra regulado en el artículo 22.4 de la Ley 3/2018, de acuerdo con el cual dicho cartel deberá informar acerca de la existencia de dicho tratamiento (videovigilancia), indicando la identidad de su responsable o del sistema de videovigilancia y la dirección del mismo. Este cartel se exhibirá en un lugar visible y, como mínimo, en los accesos a las zonas vigiladas ya sean interiores o exteriores, y en caso de que el espacio vigilado disponga de varios accesos, deberá disponerse de dicho distintivo de zona vigilada en cada uno de ellos[52]. Asimismo, por medio del referido cartel ha de darse a conocer la posibilidad de ejercitar los derechos reconocidos[53].

Los artículos 13 y 14 del RGPD convierten la obligación de información en un auténtico derecho de los interesados, directamente relacionado con la licitud del propio tratamiento. De este modo, la falta de información al interesado deviene en un incumplimiento sustancial de los principios esenciales del derecho, de suerte que se equipara la falta de información al afectado con una ausencia de base jurídica del tratamiento.[54].

---

51 Véase artículo 12.7 del RGPD.

52 MORARU, G.F., ROMERO RÓDENAS, M.J., "El deber informativo previo sobre el alcance de las medidas empresariales de videovigilancia SJS núm. 3 de Pamplona, de 18 de febrero de 2019 (sentencia núm. 52/2019)", *Revista de Jurisprudencia Laboral*- Número 2/2019.

53 Véanse los artículos 15 a 22 del RGPD.

54 PUYOL MONTERO, J., "Transparencia de la información y derecho de acceso de los interesados en la nueva normativa de protección de datos" en *Tratado de protección de datos*, Tirant Online, 2019 (TOL7218.399).

Pero a pesar de la regulación actual, existen ciertas lagunas legales como acontece en el caso de las grabaciones de empleados que cometen actos ilícitos[55]. El conflicto proviene de la redacción del artículo 89.1 de la Ley 3/2018, de 5 de diciembre, donde se regula el uso de dispositivos de videovigilancia en el lugar de trabajo, a cuyo tenor: *"los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o empleados públicos"* de dos circunstancias: la instalación de las cámaras; y del funcionamiento de estas *"para el ejercicio de las funciones de control laboral"*.

Sin embargo, su segundo párrafo dispone que *"en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica"*. Es decir, no es necesario que se haya informado al empleado que realiza el acto ilícito *in fraganti* de la concreta finalidad de control laboral, sino que basta con que sepa de la existencia de las cámaras[56].

En este sentido, pudiera parecer lógico pensar que el deber de buena fe del empresario ha de primar sobre su deber de vigilar, y solo en el supuesto de que tras, haber informado de forma correcta el trabajador, siguiera realizando conductas ilícitas, entonces sí se podría ejercer la potestad sancionadora[57].

Con todo, lo cierto es que el TEDH se ha pronunciado sobre esta controversia, produciéndose un cambio sustancial. La Gran Sala del Tribunal Europeo de Derechos

---

55 Sobre esta cuestión se pronuncia un juzgado de Pamplona, el cual rechaza la existencia de un régimen más laxo en el caso de "actos ilícitos". El juez que dicta la sentencia considera que la "contradicción" entre los párrafos primero y segundo del artículo 89 debe resolverse haciendo una interpretación proteccionista con los derechos del trabajador, "excluir la exigencia informativa de la finalidad de la videovigilancia, que forma parte del contenido esencial del derecho fundamental a la protección de datos personales, supone que la ley orgánica no está respetando el derecho a la privacidad y a la protección de datos personales conforme a la doctrina del TEDH"; de esta forma, el juzgador recuerda que la prevalencia de la legislación y jurisprudencia europeas sobre la normativa nacional y considera que, aunque el tenor literal de la ley orgánica rebaje las exigencias de información en caso de actos irregulares del empleado, se impone una interpretación más garantista, debiendo mantener los mismos requisitos que para las situaciones en las que no medien delitos o actos ilícitos. Vid. Sentencia del 8 de febrero de 2019, Juzgado de lo Social nº3 de Pamplona/Iruña (ECLI:ES:JSO:2019:28152)

56 Esta regulación legal supone que, en principio, si las cámaras de vigilancia captan actos ilícitos flagrantes la prueba obtenida es válida, aunque no se haya cumplido con las exigencias del deber informativo y sólo figure el dispositivo que indica que se trata de una *"zona videovigilada"*. Ello supondría que el trabajador a quien se refiera la grabación y que realizó el acto ilícito podrá ser sancionado.

57 GALLARDO MOYA R., "Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la sentencia del Tribunal Europeo de Derechos humanos (Gran Sala) de 5 de septiembre de 2017 en el caso Bârbulescu II c. Rumania", *Revista de Derecho Social,* núm. 79, 2017, pp. 141 a 156; PRECIADO DOMENECH C.H., "Comentario de urgencia a la STEDH 9 de enero de 2018", *Revista Información Laboral*, núm. 1, 2018.

Humanos, de 17 octubre 2019[58], hace unos pocos meses, ha revocado una Sentencia previa de Sala de 9 enero 2018[59], modificando así, su criterio respecto a la utilización por parte de las empresas de las cámaras de videovigilancia destinadas a controlar el comportamiento de sus empleados sin informar previamente de su existencia. Considera el TEDH que la instalación de estos dispositivos sin informar previamente a los empleados sometidos a videovigilancia no vulnera el derecho a la intimidad y la privacidad consagrado en la Convención Europea de Derechos Humanos (CEDH), siempre y cuando el uso de las cámaras se fundamente en la "*sospecha razonable*" de la comisión de actos ilícitos y cause perjuicio importante para la empresa[60], y que la medida se aplique de forma proporcionada.

Para ello, el TEDH recurre a los criterios utilizados en el asunto Barbulescu[61] para analizar la validez del control; en concreto:

- El grado de intromisión del empresario. El TEDH considera que la invasión de la vida privada de los empleados no se ve afectada siempre y cuando la instalación de las cámaras se limite a las zonas de trabajo donde el grado de intimidad que el empleado puede alcanzar es reducida.

- Alegación de un argumento legítimo por parte del empresario que justifique la medida.

- Existencia de medios menos intrusivos para la consecución del mismo objetivo. El TEDH entiende que ninguna otra medida puede alcanzar la finalidad deseada.

- Utilización por parte de la empresa del resultado de la medida de vigilancia. Las grabaciones no deberán ser destinadas a un fin diferente al objetivo perseguido.

---

58 Vid. STEDH de 17 de octubre de 2019 (ECLI:CE:ECHR:2019:1017JUD000187413).

59 Ello con fundamento en el artículo 43 del Convenio Europeo de Derechos Humanos. En ella se había dado la razón a las trabajadoras despedidas, teniendo en cuenta que la Sala de lo Social del Tribunal Superior de Justicia de Cataluña, confirmando Sentencia de Juzgado de lo Social, había declarado procedentes los despidos de las trabajadoras implicadas, y además, que tanto el Tribunal Supremo como el Tribunal Constitucional habían inadmitido los recursos de casación para la unificación de doctrina y de amparo, respectivamente. Vid. STSJ CAT 4294/2017, de 12 de junio (ECLI: ES:TSJCAT:2017:4294). ROJO TORRECILLA, E., "Derecho del trabajador a la privacidad de la empresa y límites a su control por cámaras de vigilancia. Estudio del caso López Ribalda y otras contra España", *Derecho de las relaciones laborales*, nº 2, 2018, pp. 137-145.

60 BLASCO JOVER, C., "Trabajadores "transparentes": la facultad fiscalizadora del empresario vs. Derechos fundamentales de los trabajadores", *Revista Internacional y comparada de Relaciones Laborales y Derecho del empleo,* Adapt University Express, 2018, pp. 48 y ss.

61 Vid. STEDH 5 de septiembre de 2017 (ECLI:CE:ECHR:2017:0905JUD006149608).

Así las cosas, a pesar de que tras la STEDH de 17 octubre 2019, el criterio del uso de las cámaras ocultas se vea reforzado, se debe aclarar que su utilización debe ser limitada en el tiempo y no debe extenderse por un periodo tan prolongado que se convierta en un sistema de carácter fijo, ya que así no se estarían cumpliendo los criterios establecidos. Por ello, sólo deben colocarse para el fin concreto y usarse para confirmarlo o no, durante un tiempo prudencial y de una manera proporcionada a la gravedad del hecho, sin que pueda exonerarse del derecho fundamental a la información.

2. Derecho de acceso de los interesados

El derecho de acceso es uno de los derechos mencionados expresamente en el apartado 2 del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, de acuerdo con el cual: "*toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación*". Se trata de un derecho esencial, debido a que el interesado debe poder saber si sus datos personales están siendo tratados, en el caso concreto el trabajador tendrá derecho a saber de la instalación de los sistemas de videovigilancia. En este sentido, el TJUEha reconocido al derecho de acceso una función instrumental en relación con los demás derechos reconocidos en el RGPD[62] ; de ahí que deba "materializarse en un modo que permita verificar al interesado que el tratamiento cumple con la legalidad y en su caso ejercer los derechos de 16 al 22"[63].

El derecho de acceso viene regulado en al artículo 15 RGPD[64]. Cuando el interesado ejercite su derecho de acceso, el responsable del tratamiento deberá confirmarle, en primer lugar, si se están tratando o no sus datos[65]. En caso afirmativo, el responsable deberá proporcionarle al interesado el acceso a sus datos y la información sobre su tratamiento cuyo contenido es prácticamente coincidente con el establecido en los artículos 13 y 14 del RGPD para el derecho de información excepción hecha de la referencia a la base jurídica del tratamiento y el interés legítimo[66].

---

62 STJUE C-553/07, de 7 de mayo (ECLI:EU:C:2009:293).

63 HERNANDEZ CORCHETE, J.A.: "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos"; en PIÑAR MAÑAS, J. L. (Dir.): *Reglamento General de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, p. 224.

64 A efectos interpretativos también han de tenerse en cuenta los considerandos 63 y 64 del RGPD.

65 El derecho de acceso y las particularidades en relación con su ejercicio está previsto en el artículo 13 de la Ley Orgánica 3/2018, de 5 de diciembre.

66 En concreto el responsable del tratamiento deberá informar sobre: los fines del tratamiento; las categorías de datos personales; los destinatarios, en particular destinatarios en terceros países u

El derecho de acceso se entenderá otorgado en el momento en que se facilite por el responsable del tratamiento un sistema de acceso remoto, directo y seguro a los datos personales, que garantice, de modo permanente, el acceso a su totalidad.

Respecto al modo en el que se debe facilitar el acceso, el artículo 15.3 del RGPD señala que se deberá facilitar una copia de los datos objeto de tratamiento de forma sencilla o con facilidad en intervalos de plazo razonables, con el fin de que el interesado pueda verificar y conocer la licitud del tratamiento.

Así las cosas, cabría plantearse si el derecho a obtener copia de los datos personales podría perjudicar a terceros. Sin embargo, el legislador, ya en el apartado 4º del artículo 15 del RGPD, prevé esta circunstancia y establece la existencia de limitaciones a su ejercicio, salvaguardando así los derechos de terceras personas.

3. Derecho de rectificación

El derecho de rectificación se encuentra mencionado en el artículo 8.2 de la Carta de Derechos Fundamentales de la Unión Europea y en el artículo 16 del RGPD, que establece que *"el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional."* De esta manera, una vez identificado el dato erróneo, este debe ser corregido, actualizado o completado para que responda a la realidad de su titular.

Existe una vinculación directa entre el derecho de rectificación y el carácter incompleto de los datos. De ahí que, por una parte, sea obligación de los responsables que los datos no sean incompletos y asimismo garantizar su actualización sin dilación indebida, y al mismo tiempo el interesado tenga el derecho a que sus datos sean rectificados en los supuestos en que sean inexactos.

organizaciones internacionales; el plazo previsto de conservación o, de no ser posible, los criterios utilizados para determinar este plazo; la existencia del derecho a solicitar la rectificación o supresión o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; el derecho a presentar una reclamación ante una autoridad de control; si los datos personales no se han obtenido del interesado, cualquier información disponible sobre su origen; la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22 (cfr. art.15 RGPD).

4. Derecho de supresión

El derecho de supresión, o también comúnmente conocido como "al olvido", se recoge en el artículo 17 del RGPD donde se establece el derecho del interesado a obtener sin dilación indebida del responsable del tratamiento la supresión de sus datos personales.

El derecho al olvido digital es una manifestación directa de los principios de minimización de datos y limitación de la finalidad, que exige la cancelación de los datos personales que ya no sean necesarios para la realización de la finalidad determinada que motivó su recogida y tratamiento[67].

La obligación de suprimir los datos personales del interesado debe cumplirse cuando se de alguna de las circunstancias recogidas en el artículo 17 del RGPD:

> *"- Cuando el interesado retire el consentimiento y este no se base en otro fundamento jurídico o cuando se oponga al tratamiento;*
>
> *- Si existe una obligación legal de suprimirlos;*
>
> *- Cuando los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información."*

Y esta se completa con una segunda obligación, recogida en el apartado segundo del artículo 17, en virtud de la cual el responsable del tratamiento, cuando haya hecho públicos los datos y esté obligado a suprimirlos, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas para informar a los responsables de la solicitud del interesado de supresión de cualquier enlace a sus datos personales, o cualquier copia o replica de los mismos[68].

El derecho a la supresión no es un derecho absoluto, pues el apartado 3 del artículo 17 establece que no será de aplicación lo dispuesto en los apartados anteriores cuando el tratamiento sea necesario:

> *"a) para ejercer el derecho a la libertad de expresión e información;*
>
> *b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o*

[67] Y es que el simple paso del tiempo puede convertir en inadecuado un tratamiento de datos inicialmente legítimo. Así lo ha entendido el TJUE en su sentencia de 13 de mayo (ECLI:EU:C:2014:317).

[68] ADSVARA, B., "Derechos de rectificación y supresión (olvido) y portabilidad (de los datos) y de limitación y oposición (al tratamiento"), en *Tratado de protección de datos*, Tirant Online, 2019 (TOL7218.402).

para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento;

e) para la formulación, el ejercicio o la defensa de reclamaciones."

5. Otros derechos

5.1. Derecho a la limitación del tratamiento

El derecho a la limitación del tratamiento se encuentra recogido en el art. 18 del RGPD. Se podrá solicitar esencialmente en los supuestos en que "el tratamiento de los datos es ilícito, y por tanto el interesado necesita que se mantenga la prueba de dicho incumplimiento para que la misma no desaparezca, o el interesado necesita que se mantengan los datos personales, incluso después de que se haya cumplido la finalidad del tratamiento, para presentar, ejercer o defenderse en reclamaciones"[69].

La limitación del tratamiento viene definida en el artículo 4.3. del RGPD como *"el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro"*; y supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

5.2. Derecho de oposición

Conforme a lo dispuesto en el artículo 21 del RGPD el interesado también tiene derecho a oponerse al tratamiento de sus datos en varios supuestos. En concreto, así acontece:

En primer lugar, por motivos relacionados con la situación particular del interesado cuando el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (cfr. art. 6.1.e. RGPD), o cuando el tratamiento es necesario

[69] RECIO GAYO, M.: "Los nuevos y renovados derechos en Protección de Datos en el RGPD, así como sus limitaciones", *Actualidad Civil* núm. 5, mayo, 2018.

para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero (cfr. art. 6.1.f. RGPD), incluida la elaboración de perfiles sobre la base de dichas disposiciones[70].

En segundo lugar, el interesado, también por motivos relacionados con su situación particular, podrá oponerse al tratamiento de sus datos personales con fines de investigación científica o histórica o fines estadísticos de acuerdo con lo establecido en el artículo 89.1 del RGPD, salvo que el tratamiento sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Y en tercer lugar, el interesado podrá oponerse al tratamiento de datos con fines de mercadotecnia directa, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

5.3. Derecho a la portabilidad de los datos

El derecho de portabilidad de los datos se encuentra recogido en el artículo 20 del RGPD y en el artículo 17 de la Ley 3/2018, de 5 de diciembre con una remisión directa y sin especificaciones al citado precepto del RGPD. Su razón de ser es "reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados"[71].

Establece el artículo 20 del RGPD que el interesado tendrá derecho a recibir del responsable del tratamiento los datos personales que le incumban en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable cuando:

> *"a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y*
>
> *b) el tratamiento se efectúe por medios automatizados."*

[70] ÁLVAREZ CARO, M.: "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", en PIÑAR MAÑAS, J. L. (dir.): *Reglamento General de protección de datos*…, ob. cit., p. 236.

[71] Véase el considerando 68 del RGPD.

V. EL RÉGIMEN SANCIONADOR

Cuando la instalación de sistemas de videovigilancia se realiza sin cumplir los requisitos exigidos, el trabajador ve vulnerados sus derechos fundamentales, de forma que podrá dirigirse a los tribunales del orden social, si así lo considera; o incluso dirigirse al orden penal, siempre y cuando la grabación fuese constitutiva de delito, por enfocar en lugares prohibidos.

Con todo, cabe decir que los Tribunales, en ocasiones, han admitido la instalación de forma oculta de mecanismos de captación de imágenes y sonidos sin haber realizado la oportuna comunicación a los trabajadores o a sus representantes legítimos[72], sin cumplir, por tanto, lo preceptuado en el artículo 64.1ET, de acuerdo con el cual: *"El Comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores..."*.

El uso de un sistema de videovigilancia para un control laboral, cuyo único fin fuera la seguridad de los bienes y las personas, constituye una desviación de la finalidad, y en consecuencia, supone una infracción tipificada en el RGPD. Lo que se pretende con las sanciones es lograr una protección efectiva de los datos de carácter personal, y reforzar tanto los derechos de los interesados como las obligaciones de las empresas que traten los datos personales[73].

En el capítulo VIII del RGDPD se establece que cualquier ciudadano europeo que considere que se ha vulnerado su derecho fundamental a la protección de datos y tenga pruebas de ello, puede ponerlo en conocimiento del organismo competente con el fin de que cese la infracción y se sancione al infractor[74].

El artículo 83 RGPD recoge las condiciones generales para la imposición de multas de carácter administrativo. De entrada, debe significarse que cada autoridad de control deberá garantizar que la imposición de multas sea en cada caso individual, efectiva, proporcionada y disuasoria[75].

---

[72] En este sentido, resulta ilustrativa la STEDH de 17 de octubre de 2019 (ECLI:CE:ECHR:2019:1017JUD000187413).

[73] FABREGAT MONFORT, G., *Nota Resumen de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Tirant Online, 2018.

[74] Véase el artículo 77 RGPD: *"(...) todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento."*

[75] El RGPD faculta a cada Autoridad de Control para la fijación de los criterios y de la cuantía de las multas administrativas en cada caso y de forma particular. Los criterios estarán basados en la naturaleza, gravedad y duración de la infracción y sus consecuencias y las medidas tomadas para garantizar el

Además, la imposición de una multa y su cuantía supone la toma en consideración de todas las circunstancias concurrentes en el caso individual; así, entre otras, la naturaleza, gravedad y duración de la infracción y sus consecuencias; las medidas adoptadas para garantizar el cumplimiento de las obligaciones impuestas por el Reglamento e impedir o mitigar las consecuencias de la infracción, o la intencionalidad o negligencia en la infracción.[76].

En este orden de ideas, partiendo en la base de que el RGPD establece un sistema de sanciones que permite un amplio margen de apreciación, la LOPDGDD en su Título IX describe, con mayor concreción, las conductas típicas o infracciones, las sanciones, los plazos de prescripción de unas y otras, así como los sujetos responsables. Mas debe tenerse en cuenta que la categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, Y es que el Derecho de la Unión Europea no admite la tipificación y clasificación de las infracciones por cada Estado miembro, pues con ello se rompería la unificación del régimen sancionador a nivel europeo[77].

Por lo que respecta a las infracciones, estas se clasifican en: muy graves, graves y leves y prescriben a los 3, 2 y 1 años, respectivamente.

- Las infracciones muy graves se encuentran reguladas en el artículo 72 de la LOPDGDD: son aquellas que suponen una vulneración sustancial del tratamiento, en función de lo establecido en el art. 83.5 del RGPD, y que tienen que ver con el uso de los datos para una finalidad diferente de la indicada, o entre otras, con la vulneración del deber de confidencialidad del artículo 5 de la LOPDGDD.

- Las infracciones graves son las previstas en el artículo 73 de la LOPDGDD: se trata de aquellas que suponen la vulneración sustancial del tratamiento, en función de lo establecido en el art. 83.4 del RGPD, y guardan relación con la falta de adopción de medidas técnicas y organizativas necesarias para la efectiva protección de datos.

- Las infracciones leves están reguladas en el artículo 74 de la LOPDGDD: son aquellas de carácter meramente formal; es decir, el resto de infracciones que no estén contempladas en las dos anteriores categorías. Entre ellas podemos encontrar supuestos

---

cumplimiento de las obligaciones impuestas por la normativa e impedir o mitigar las consecuencias de la infracción.

[76] Véase artículo 84.1. RGPD: *"Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias."*

[77] TERRON SANTOS, D., DOMINGUEZ ALVAREZ, J.L., "Protección de datos y derechos digitales", *Crónica de legislación Administrativo Ars Iuris Salmanticensis*, vol. 7, 2019, p. 236.

tales como la falta de transparencia de la información o la infracción del derecho de información del afectado.

El RGPD establece un sistema dual para fijar la cuantía de las sanciones. En el caso de las infracciones muy graves impone multas administrativas que pueden alcanzar los veinte millones de euros o, tratándose de una empresa, de una cuantía equivalente al 4% de la facturación. Para fijar este importe se basa en el incumplimiento de los principios básicos de tratamiento, la vulneración de los derechos de los interesados, en la transferencia a terceros países y en el incumplimiento de una resolución[78].

Y en el supuesto de las infracciones graves se sancionarán con multas administrativas que puedan ascender hasta los diez millones de euros o, si se trata de una empresa, una cuantía máxima del 2 % de la facturación. Estas cuantías se impondrán cuando se produzca una vulneración de las obligaciones del responsable y del encargado o cuando no se cumplan las obligaciones de certificación, ni de control[79].

En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento[80].

El legislador ha pretendiendo que las empresas se vean obligadas a cumplir puntualmente con la normativa de protección de datos ya que como ciudadanos de la Unión Europea tenemos el derecho a tener nuestra privacidad bajo control.

La LOPDGDD mantiene la distinción entre infracciones muy graves, graves y leves con la imposición de diferentes cuantías en función de: el carácter continuado de la infracción, la vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal, los beneficios obtenidos como consecuencia de la comisión de la infracción, la posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción y la existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente[81].

Las sanciones parecen elevadas, pero estas son aplicadas en función de la gravedad de cada caso en concreto y dentro del marco de la legalidad. Por ello, los empresarios deben preocuparse de cumplir las obligaciones que establece la normativa, en los supuestos de tratamiento de los sistemas de videovigilancia, y garantizar así la protección de los datos personales de sus trabajadores.

---

78 Véase el artículo 83.5 del RGPD.

79 Véase artículo 83.4 del RGPD.

80 Tal y como se describe en el Considerando 148 del RGPD.

81 Véase el artículo 76. 2 de la Ley 3/2018, de 5 de diciembre.

CONCLUSIONES

PRIMERA.- La videovigilancia es un proceso por el cual es posible obtener imágenes de personas y objetos en base a una finalidad específica, la de salvaguardar la seguridad tanto de bienes como de personas.

Su uso en el entorno empresarial determina si los trabajadores cumplen o no sus obligaciones laborales.

En la práctica viene a significar que los empleadores contarían con información de carácter personal de los empleados, y una gestión incorrecta de los datos recolectados por los sistemas de videovigilancia, podría dar lugar a una vulneración de los derechos de los trabajadores, más concretamente del derecho a la intimidad personal y su propia imagen por lo que es fundamental la protección frente al uso de los datos de carácter personal.

SEGUNDA.- Por ello, es necesario que el uso de la información recogida mediante sistemas de videovigilancia sea proporcional al fin con el que fueron instalados y no de manera discriminatoria que ejerza un control directo de los trabajadores.

Para que esto suceda, los trabajadores cuentan con una serie de garantías reguladas en la RGPD con respecto al tratamiento de la información recolectada, que no debe recogerse bajo ningún tipo de engaño ni de manera fraudulenta, y en todo caso deberá utilizarse de manera racional.

TERCERA.- Además, como el propósito del uso de los datos debe ser claro y determinado de antemano por el empleador, no pueden utilizarse más allá del objetivo establecido y deben estar estrictamente limitados al susodicho fin. En este sentido, no solo deben utilizarse de manera diligente y ser en todo caso correctos, completos y actuales, sino que también deben conservarse únicamente el tiempo necesario para la finalidad con la que se recogen, por lo que la información debe ser estrictamente confidencial.

CUARTA.- Llegados a este punto, cabe plantearse a qué medidas de seguridad debe atenerse el empleador, y si bien el RGPD no establece una lista exhaustiva de las mismas, si deja claro que deben ser medidas consideradas adecuadas y proporcionadas tras la ponderación del riesgo que supone el uso de la información recolectada mediante los sistemas de videovigilancia, teniendo siempre en cuenta los riesgos de probabilidad y gravedad tanto de los derechos como de las libertades de las personas. Para ello, las empresas suelen utilizar los “Códigos de conducta” con los que vienen a adoptar un comportamiento ético para la no vulneración de estos derechos.

QUINTA.- Es gracias a estos Códigos de conducta que las empresas establecen los limites y los plazos para el uso de los datos. De esta manera, es obligatorio informar a los trabajadores la finalidad de la obtención de los datos. Este deber, tanto de información como de transparencia, se encuentra recogido y regulado en el RGPD y ha generado cierta controversia.

SEXTA.- En cuanto al derecho de información, tras estudiar la diversidad de jurisprudencia llegamos a la conclusión de que el empresario debe informar, con carácter previo a la puesta en funcionamiento del sistema, sobre la finalidad de control empresarial de la captación de imágenes a los trabajadores y a la representación sindical, por cualquier medio que garantice la recepción de la información. Y en el caso de que se capte la comisión flagrante de un acto ilícito por los trabajadores, o se tenga la *"sospecha razonable"*, no será necesaria la información previa y se entenderá cumplido el deber de informar cuando existiese al menos el cartel informativo en lugar suficientemente visible identificando.

Asimismo, pondrá a disposición de los trabajadores toda la información del artículo 13 del RGPD y, finalmente, se habrá de colocar 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 de protección de datos y dónde obtener más información sobre el tratamiento de los datos personales. La instalación de sistemas de grabación de sonidos y de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos, queda terminantemente prohibida.

SÉPTIMA.- No cabe duda que con el régimen sancionador resultará conveniente que las empresas revisen sus actuaciones y medidas de seguridad en materia de protección de datos, para evitar así las sanciones de cuantías elevadas.

OCTAVA.- Ni la regulación normativa ni la interpretación judicial han logrado generar un marco sólido para la aportación de imágenes extraídas de sistemas de videovigilancia con fines de control laboral, pero sí han contribuido a establecer unas bases mínimas para garantizar la licitud de las medidas de control y la efectividad de los derechos fundamentales de los trabajadores.

BIBLIOGRAFÍA CONSULTADA

- ADSVARA, B., "Derechos de rectificación y supresión (olvido) y portabilidad (de los datos) y limitación y oposición (del tratamiento)", en *Tratado de protección de datos,* Tirant Online, 2019.

- ALVAREZ, CARO, M., "El derecho de rectificación cancelación limitación del tratamiento, oposición y decisiones individuales automatizadas", en PIÑAR MAÑAS, J.L., (Dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad.* Editorial Reus, Madrid.

- BLASCO JOVER, C., "Trabajadores "transparentes": la facultad fiscalizadora del empresario vs. Derechos fundamentales de los trabajadores", *Revista Internacional y comparada de RELACIONES LABORALES Y DERECHO DEL EMPLEO,* Adapt University Express.

- CALONGE CRESPO, I., "Videovigilancia y seguridad pública", en ETXBERRIA GURIDI, J.F., *Videovigilancia: ámbito de aplicación y derechos fundamentales afectados,* Ed. Tirant lo Blanch, 2010.

- CUEVA CALABIA, J.L., "La LORTAD y la seguridad de los sistemas automatizados de datos personales", *Actualidad Informática Aranzadi*, núm. 13, octubre, Aranzadi, 1994.

- DEL PESO NAVARRO, E., RAMOS GONZALEZ, M.A., DEL PESO RUIZ, M., y DEL PESO RUIZ, M., "*Nuevo Reglamento de Protección de datos de carácter personal: medidas de seguridad*", Ediciones Díaz de Santos, 2012.

- PUENTE ESCOBAR, A., 8ª Sesión anual abierta de la AEPD. Gran Auditorio Ramón y Cajal, 29 de junio de 2016.

- PUENTE ESCOBAR, A., "Principios y licitud del tratamiento" en *Tratado de protección de datos,* Tirant Online, 2019.

- FABREGAT MONFORT, G., *Nota Resumen de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales,* Tirant Online, 2018.

- GALLARDO MOYA, R., "Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de septiembre de 2017 en el caso Bârbulescu II c. Rumania", *Revista de Derecho Social,* nº 79, 2017.

- GOÑI SEIN, J.L., *La videovigilancia empresarial y la protección de datos personales*, Thomson-Aranzadi, Pamplona, 2007.

- GRAFENSTIN, M. V., "*The Principle of Purpose Limitation in Data Protection Laws*", Nomos, 2018.

- HERNANDEZ CORCHETE, J.A., "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos", en PINAR MAÑAS, J.L., (Dir.), *Reglamento general de Protección de datos. Hacia un nuevo modelo europeo de privacidad.* Editorial Reus, Madrid.

- MORARU, G., F., ROMERO RÓDENAS, M.J., "El deber informativo previo sobre el alcance de las medidas empresariales de videovigilancia SJS núm. 3 de Pamplona de 18 de febrero de 2019 (sentencia núm. 52/2019)", *Revista de Jurisprudencia Laboral,* número 2/2019.

- RALLO LOMBARTE, A., "Del derecho a la protección de datos a la garantía de nuevos derechos digitales", en *Tratado de protección de datos,* 2019, Tirant Online (TOL7218.393).

- REBOLLO DELGADO, L., SERRANO PEREZ, M.M., *Introducción a la protección de datos*, Dykinson, Madrid, 2008.

- RECIO GAYO, M., "Los nuevos y renovados derechos en protección de datos en el RGPD, asi como sus limitaciones", *Actualidad Civil* núm.5, mayo, 2018.

- ROJO TORRECILLA, E., "Derecho del trabajador a la privacidad de la empresa y límites a su control por cámaras de vigilancia. Estudio del caso López Ribalda y otras contra España", *Derecho de las relaciones laborales*, núm. 2, 2018.

- ORDEÑANA GEZURAGA, I., "La videovigilancia en el ámbito laboral. Especial incidencia en su utilización en el proceso laboral" en ETXBERRIA GURIDI, J.F., *Videovigilancia: ámbito de aplicación y derechos fundamentales afectados*, Ed. Tirant lo Blanch, 2010.

- PRECIADO DOMENECH, C.H., "Comentario de urgencia a la STEDH 9 de enero de 2018", *Revista Información Laboral*, nº 1, 2018.

- PUYOL MONTERO, J., "Transparencia de la información y derecho de acceso de los interesados en la nueva normativa de protección de datos", en *Tratado de protección de datos,* Tirant Online, 2019.

- SAIZ PEÑA, C.A., "Seguridad de los datos, evaluación de impacto, códigos de conducta y certificaciones", en *Tratado de protección de datos,* Tirant Online, 2019.

- SANCHEZ-RODAS NAVARRO, C., "Videocámaras y poder de vigilancia", *Aranzadi social*, núm.5, tomo 9, 1999.

- TERRON SANTOS, D., DOMINGUEZ ALVAREZ, J.L., "Protección de datos y derechos digitales", *Crónica de legislación Administrativo Ars Iuris Salmanticensis*, vol. 7, 2019.

- VALDECANTOS, M., "El consentimiento como base legitimadora del tratamiento en el Reglamento europeo de protección de datos", *Actualidad Civil*, núm.5, mayo, 2018.

COMPENDIO NORMATIVO

- Convenio de Roma de 4 de noviembre de 1950, para la protección de los derechos humanos y de las libertades fundamentales.

- Constitución española de 1978.

- Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

- Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.

- 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 videocámaras.

- Carta de los derechos fundamentales de la Unión Europea (entrada en vigor 1 de diciembre del 2009).

- Ley 5/2014, de 4 de abril, de seguridad privada.

- 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.

- Directiva 2016/680, de la Unión Europea de 27 de abril de 2016.

- Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

- Ley Orgánica 3/2018, de 5 de diciembre de Protección de datos personales y garantía de los derechos digitales.

COMPENDIO JURISPRUDENCIAL

SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL

- STC 254/1993, de 20 de julio (ECLI:ES:TC:1993:254)

- STC 98/2000, de 10 de abril (ECLI:ES:TC:2000:98)

- STC 186/2000, de 10 de julio (ECLI:ES:TC:2000:186)
- STC 81/2001, de 26 de marzo (ECLI:ES:TC:2001:81)
- STC 292/2000, de 30 de noviembre (ECLI:ES:TC:2000:292)
- STC 70/2009 de 22 de abril (ECLI:ES:TC:2009:70)

SENTENCIAS DEL TRIBUNAL SUPREMO

- STS 545/2013 de 29 de enero (ECLI:ES:TS:2013:545)

SENTENCIAS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

- STJUE C-553/07, de 7 de mayo (ECLI:EU:C:2009:293)
- STJUE 317/2014 de 13 de mayo (ECLI:EU:C:2014:317)
- SETDH de 9 de enero (ECLI:CE:ECHR: 2018:0109JDU000187413)
- STEDH de 17 de octubre (ECLI:2019:1017JUD000187413)

OTRAS SENTENCIAS

- STSJ CAT 4294/2017, de 12 de junio (ECLI:ES:TSJCAT:2017:4294)
- SAN 4202/2011, de 22 de septiembre (ECLI:AN:2011:4202)
- Sentencia de 8 de febrero del 2019, Juzgado de lo Social nº3 de Pamplona/Iruña (ECLI:ES:JSO:2019:28152)