Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Asesoría Jurídica de Empresas

LA ÉTICA DEL RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES EN LAS RELACIONES LABORALES: SISTEMAS DE VIDEO-VIGILANCIA.

Trabajo fin de estudio presentado por:	Carlos Morato Roig
Tipo de trabajo:	Investigación teórica
Director/a:	Rolando Ortega Hernández
Fecha:	15/09/2021

Resumen

El uso progresivo de las nuevas tecnologías en la vida diaria de los ciudadanos ha generado una serie de situaciones que potencialmente atentan contra los derechos fundamentales de los ciudadanos. Sin embargo, durante la última década, las instituciones europeas y el legislador español han conseguido un notable avance en los derechos sociales y laborales de los trabajadores con la publicación del reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos, respectivamente. Es por ello que este trabajo pretende esclarecer la ética y la responsabilidad del Responsable del tratamiento de datos personales en las relaciones laborales centrando el estudio en los sistemas de video-vigilancia. Asimismo, tras haber analizado la normativa y la jurisprudencia de los tribunales, así como las resoluciones de organismos de protección de datos y bibliografía de expertos, se trata de poner de relieve el amparo de los derechos de los trabajadores en materia de protección de datos.

Palabras clave: *video-vigilancia; trabajador; datos personales; Responsable del tratamiento; protección de datos.*

Abstract

The progressive use of new technologies in our daily life has created a series of situations that potentially might threaten our fundamental rights. However, during the last decade, European institutions and the Spanish legislation have accomplished a notable progress regarding workers' social and labour rights with the Publication of the *General Data Protection Rules and the Organic Law of Data Protection*, respectively. Therefore, this work intends to establish the ethic and the responsibility of the person responsible of personal data treatment regarding labour relationships focusing the study on the video monitoring system. Moreover, after analysing the regulations and jurisprudence of the courts, like data protection organisms' resolution, it's about emphasising workers' rights protection with respect to data protection.

Keywords: *video monitoring, worker, personal data, data treatment responsible, data protection.*

Índice de contenidos

1. Introducción

1.1. Justificación del tema elegido

El Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016[1] (en adelante, RGPD) significó un gran paso adelante para la protección de la privacidad de los ciudadanos de Europa en un momento de la historia en que el almacenamiento de datos personales se había convertido en un verdadero peligro para las libertades individuales en favor de grandes empresas.

Posteriormente, la adaptación de dicho Reglamento al ordenamiento jurídico español mediante la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[2] (en adelante, LOPD), ha supuesto un claro avance para el amparo de los trabajadores en tanto que se han estipulado ciertos límites empresariales al control por medio de sistemas de video-vigilancia y de grabación.

En ese sentido, los derechos laborales se han visto ampliados atendiendo a las necesidades generadas por la sociedad de la información del siglo XXI. Sin embargo, el uso excesivo de las TICs (Tecnologías de la Información y Comunicación) la vida diaria sitúa a los trabajadores de forma particular y a toda la ciudadanía en general en una situación de continuo peligro por la vulneración de derechos derivados de la protección de datos personales.

Si bien es cierto que la Ley regula quién es el responsable del tratamiento de la protección de datos y quién el delegado y, a su vez, contempla las funciones que tienen cada uno de ellos, los trabajadores en innumerables ocasiones deben hacer un acto de fe y confiar en que los datos facilitados van a ser correctamente tratados. No obstante, ¿qué ocurre con el registro de imágenes y de sonido mediante el sistema de video-vigilancia? Los trabajadores son conocedores de los datos que ofrecen expresamente pero no de aquellas imágenes y sonidos que se dan durante el día a día.

[1] DOUE L.119/1 (04-05-2016)
[2] BOE. Núm 294 (06-12-2018)

Asimismo, se debe recordar que el Derecho del Trabajo está pensado, sobre todo, para garantizar al trabajador unas condiciones mínimas para la prestación de sus servicios a cuenta ajena. Por lo tanto, la protección de datos personales debe ser uno de los derechos que garanticen mediante la colaboración, en este caso, del responsable y del delegado de protección de datos.

1.2. Problema y finalidad del trabajo

Los datos personales y la información en general se han convertido en una mercancía muy preciada por las empresas, sobre todo, tecnológicas. Sin embargo, no sólo se obtienen datos personales con la utilización diaria del teléfono móvil o de las redes sociales, sino que incluso en el puesto de trabajo se puede obtener información de los trabajadores sin que se den cuenta. Cierto es que para poder conseguir datos personales se debe consentir de forma expresa. Sin embargo, los trabajadores se olvidan fácilmente de que mediante el uso de sistemas de video-vigilancia y de grabación de sonidos instalados en las empresas donde prestan servicios se están obteniendo datos (imágenes y sonidos) personales.

Ante el desconocimiento generalizado del contenido de este tipo de derechos y la promulgación del RGPD y, posteriormente, la adaptación de dicho Reglamento en España a través de la LOPD, las empresas han visto limitado el uso indiscriminado del registro de imágenes y de sonidos de los trabajadores. Es en ese punto donde se debe incidir más sobre el papel que juegan el responsable del tratamiento de datos personales y el correspondiente delegado de protección de datos.

Si bien es cierto que tanto el responsable como el delegado de protección de datos deben ser los garantes de que los derechos de los trabajadores en este ámbito no se vean vulnerados, ¿qué ocurre cuándo no actúan como prevé la ley? ¿Cómo podrían ver resarcidos los trabajadores la vulneración de sus derechos en relación con la protección de datos?

1.3. Objetivos

El objetivo que se plantea con la realización de este Trabajo de Final de Máster (en adelante, TFM) es despejar las dudas que pudieran existir en torno a los límites del uso de las imágenes conseguidas a través de sistema de video-vigilancia.

En primer lugar, se determinará por qué son sujetos interesados tanto los trabajadores como las empresas para la consecución de una verdadera protección de datos y los riesgos que podrían asumir en el ejercicio de sus funciones.

De igual modo, se estudiará el papel determinante que juegan el responsable del tratamiento, así como el encargado del tratamiento de datos personales en las relaciones laborales y más concretamente en la aplicación de sistemas de video-vigilancia y grabación de sonidos. Es por ello que se analizará la licitud y la proporcionalidad de la aplicación de dichos sistemas, así como los derechos de los que dispondrán los trabajadores como afectados y las obligaciones de las empresas como responsables del tratamiento de datos de carácter personal.

Además, se analizará si las imágenes captadas por los sistemas de video-vigilancia pueden servir para sancionar a los trabajadores y en caso de ser así, que requisitos se deben cumplir para no vulnerar los derechos de los empleados.

Asimismo, se analizará qué responsabilidad tienen los sujetos responsables del tratamiento de los datos de carácter personal de los trabajadores en relación con posibles infracciones y cómo se podrían resarcir las vulneraciones de derechos.

1.4. Metodología

El presente TFM tiene una aproximación de investigación teórica dogmática a través de la técnica documental bibliográfica. Las fuentes utilizadas para este TFM son la legislación doctrina y la jurisprudencia. En tal sentido, se estudiará la doctrina de juristas y expertos en protección de datos y se profundizará en la jurisprudencia de los tribunales españoles y europeos como también se analizarán los criterios de organismos vinculados directamente con la materia como puede ser la Agencia Española de Protección de datos (en adelante, AEPD) a través de sus circulares, informes y resoluciones.

1.5. Estructura

El trabajo se compone de tres partes claramente diferenciadas. En primer lugar, se analizará el marco normativo de la protección de datos tanto a nivel europeo como a nivel nacional, estudiando tanto la legislación vigente como las directrices y resoluciones de los organismos constituidos para velar por el cumplimiento de la normativa de protección de carácter personal.

En segundo lugar, se analizarán los actores que participan en el tratamiento de datos personales. En ese sentido, se estudiará la figura del trabajador como persona afectada en la protección de datos, la del responsable y el encargado del tratamiento y, finalmente, la del delegado de protección de datos. Dicho estudio consistirá en analizar los derechos y obligaciones de cada uno de ellos, así como los elementos esenciales para la licitud del tratamiento de datos personales de los trabajadores.

Por otro lado, el sistema de video-vigilancia y las formas de control de la empresa constituirán el núcleo principal de este trabajo, analizando la incidencia y afectación de los trabajadores ante la instalación de este tipo de control en los centros de trabajo. En ese sentido, se estudiarán los elementos necesarios para considerar la instalación de video-vigilancia como sistemas de control lícitos y proporcionales, así como los derechos y obligaciones de los trabajadores y de las empresas.

Finalmente, se indagará sobre la responsabilidad que asumen los responsables y encargados del tratamiento de datos personales desde el punto de vista de la responsabilidad civil, como también desde el punto de vista del régimen sancionador administrativo.

2. Marco teórico y desarrollo

2.1. Marco normativo

2.1.1. Normativa de la Unión Europea

La Carta de Derechos Fundamentales de la Unión Europea[3] (en adelante, CDFUE) contempla en su artículo 8 que *"...toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan…"*. Por otro lado, el Tratado de Funcionamiento de la Unión Europea[4] (en adelante, TFUE) establece que *"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"*.

Así, durante los últimos años, la protección de datos ha sido desarrollada por las instituciones europeas a fin de poder garantizar este derecho de carácter individual de los ciudadanos de la Unión. En ese sentido, y de forma más particular, gracias a la Proclamación interinstitucional sobre el pilar europeo de derechos sociales de 13 de diciembre de 2017[5] se consideró que los trabajadores tenían el derecho a proteger sus datos personales en el contexto del trabajo.

Con anterioridad a la normativa actual, el Parlamento Europeo y el Consejo promulgaron la Directiva 95/46/CE de 24 de octubre de 1995[6], la cual tenía como objetivo principal eliminar los obstáculos a la libre circulación de los datos dentro del espacio común que pudieran surgir de la protección del derecho a la protección de datos personales. Sin embargo, dicha Directiva no era traspuesta de forma homogénea en todos los Estados miembros de la Unión. Es por ello que a través del propio Tribunal de Justicia de la Unión Europea en adelante TJUE) se fue configurando una jurisprudencia que servía para interpretar tanto lo dispuesto en la mencionada Directiva como también en el artículo 8 del CEDH (TJUE 24-11-11, C-468/10 y C-469/10, ASNEF).

[3] DOCE 2000/C 364/01
[4] DOUE 2012/C 326/01
[5] DOUE 2017/C 428/09
[6] DOCE núm. 281, de 23 de noviembre de 1995. Actualmente la Directiva 95/46/CE de 24 de octubre de 1995 no está vigor desde el pasado 25 de mayo de 2018 ya que mediante el Reglamento 2016/679, de 27 de abril se derogó.

A través de la Directiva 95/46/CE se contempló la creación de un órgano independiente que dictara resoluciones de carácter no vinculante, es decir, consultivo. El Grupo del art. 29, haciendo mención a la disposición de la Directiva en el que se encuentra regulado dicho órgano, lo conforman representantes de las autoridades de protección de datos de la Unión Europea y de la Comisión teniendo como objetivo la aplicación uniforme de las medidas nacionales. Según el Dictamen 8/2001 del GT29, las funciones de dicho organismo consistían en colaborar en la aplicación de forma uniforme de las normativas y/o medidas de los Estados miembros que hubieran adoptado en base a la Directiva 95/46/CE sobre protección de datos.

No obstante, el éxito de la Unión Europea para garantizar la protección de datos de carácter personal se refleja en el RGPD. Esta norma conocida también como Reglamento General de Protección de datos, contempla en su artículo 88 la problemática existente entre la protección de datos de carácter personal y las relaciones laborales. Sin embargo, la Unión Europea consideró apropiado delegar a los Estados miembros la regulación correspondiente sobre la protección de datos de los trabajadores. De hecho, contempló la posibilidad, como se verá más adelante, que fueran los convenios colectivos los que establecieran normas más específicas para la protección de los datos personales de los trabajadores.

Con la intención de que el RGPD se aplique de acuerdo con sus disposiciones y de forma uniforme en todo el territorio comunitario, se creó el Comité Europeo de Protección de Datos cuya composición la completan los directores de las autoridades de protección de datos y el supervisor europeo de protección de datos (MERCADER UGUINA, 2019). Este organismo podrá emitir resoluciones o directrices sobre la interpretación de los conceptos derivados de la protección de datos, así como también deberá emitir decisiones vinculantes que afecten a diversos estados garantizando de tal forma que las normas comunitarias se aplicarán uniformemente.

2.1.2. Legislación española

Tal y como se ha indicado en el punto anterior, el RGPD delega la regulación de la protección de datos de los trabajadores a los Estados miembros a través de sus herramientas legislativas. Es por ello por lo que se promulgó la LOPD. El Título X de la LOPD estableció la regulación

correspondiente en materia de garantías de los derechos digitales en el ámbito de las relaciones laborales.

Gracias a la LOPD y concretamente al Título X, se ha instaurado un control del tráfico de información en la empresa que permite al trabajador prestar sus servicios sin que se vulneren derechos fundamentales y, por otro lado, el empresario ha visto regularizado el tratamiento automatizad de datos. A modo de anotación ya que más adelante este punto se va a desarrollar con mayor profundidad, particularmente, en el artículo 89 de la LOPD se contempla el derecho a la intimidad frente al uso de dispositivos de video-vigilancia y de grabación de sonidos en el lugar de trabajo.

La Agencia Española de Protección de Datos es el organismo que se encarga de supervisar la correcta aplicación de la LOPD y del RGPD y garantiza y tutela el derecho fundamental a la protección de datos. En ese sentido, la AEPD realiza también publicaciones de carácter informativo a fin de que las personas afectadas por la normativa de protección de datos conozcan cómo deben aplicarla. No es casual que la AEPD contemplara como una problemática a tratar la protección de datos en materia laboral y, por ese motivo, publicó la *Guía de la protección de datos en las relaciones laborales*.

Asimismo, no en el orden legislativo, pero sí como organismo que vela por la tutela de derechos fundamentales, el Tribunal Constitucional (en adelante TC) ha considerado la protección de datos personales como un derecho fundamental por el que se garantiza que una persona pueda controlar sus datos y el uso que se les da evitando de tal manera el tráfico ilegal de éstos. A modo de ejemplo, el fundamento jurídico (en adelante, FJ) cuarto de la sentencia del Tribunal Constitucional 94/1998 estableció unos límites al tratamiento de los datos facilitados por los trabajadores consistentes en la utilización exclusiva de los datos para la finalidad para la que se recabaron. Por otro lado, el TC en sus sentencias 29/2013 FJ (7) y 39/2016 FJ (3-4) se pronunció también sobre el alcance del derecho de información derivados del uso de sistemas de video-vigilancia. Así, según el FJ 4 de esta última sentencia, *"…el empresario no necesita del consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme al art. 20.3 ET…"* ya que considera que *"…el*

consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario…". Este aspecto, como se verá más adelante, ha sufrido diversas modificaciones y matizaciones que han pretendido conseguir un equilibrio que garantizara los derechos de las empresas y de los trabajadores.

2.1.3. Negociación colectiva

Tal y como se ha indicado anteriormente, el artículo 88 del RGPD contemplaba la posibilidad de que los convenios colectivos regularan la protección de datos en el ámbito laboral en tanto que norma más específica. Asimismo, la LOPD dispone en su artículo 91 que los convenios colectivos tienen la potestad de *"…establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral…"*.

2.2. El trabajador en la protección de datos personales.

2.2.1. El tratamiento de datos de carácter personal del trabajador.

El trabajador es considerado como sujeto titular activo en la regulación sobre la protección de datos y, por tanto, se trata de un sujeto interesado a efectos del tratamiento de datos en las relaciones laborales. En ese sentido, la AEPD reconoció que en los ficheros automatizados de personal de las empresas existen una gran cantidad de información sobre los trabajadores entre las que podemos encontrar su vida profesional, la titulación, retribución, vida familiar y, por otro lado, información más delicada como son las bajas laborales, enfermedades profesionales o, incluso, afiliaciones sindicales.

Así, para que se considere lícito el tratamiento de datos personales, el RGPD establece en su artículo 6 un listado de fundamentos jurídicos en los que se tiene que justificar dicho tratamiento y que se desarrollan a continuación.

2.2.1.1. El consentimiento como fundamento del tratamiento

El artículo 4.11 RGPD establece la definición de consentimiento del interesado la cual consiste en *"…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…"*. Atendiendo a dicha definición, si el interesado da su consentimiento para el tratamiento de datos personales para unos fines concretos se considerará lícito dicho tratamiento en tanto en cuanto el consentimiento es uno de los elementos legitimadores.

Por otro lado, la LOPD acogiendo la definición establecida por el RGPD añade que en los casos en que exista más de una finalidad se deberá hacer constar de manera específica que el consentimiento se otorga para todas las finalidades informadas. Con el objetivo de que no exista problemas posteriores al otorgamiento del consentimiento, éste deberá darse mediante un acto afirmativo claro que cumpla con lo dispuesto en la definición del consentimiento por parte del RGPD. Si bien es cierto que existen tres modos de otorgar consentimiento (expreso, tácito y presunto) sólo el consentimiento expreso es válido para garantizar la protección de datos personales. Ello es así atendiendo a lo dispuesto en el artículo 4.11 RGPD en el que hace referencia a *"…una clara acción afirmativa…"* y, por otro lado, el considerando 32 del propio Reglamento expone que *"…Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento…"*. Es decir, el consentimiento tácito entendido como aquel en el que el silencio se presume o se supone como un acto de aceptación y, por otro lado, el consentimiento presunto el cual consiste en que no se deduce ni de una manifestación ni de un acto de silencio positivo, sino a partir de una conducta, son dos tipos de consentimientos que no cumplen con lo dispuesto por la normativa que regula la protección de datos y, en consecuencia, deben ser considerados dos consentimientos inválidos a efectos de esta materia. Asimismo, la AEPD ha insistido a través de su informe 0039/2010 que el consentimiento debe ser libre, específico, informado e inequívoco.

Según el Dictamen 8/2001 del Grupo del art. 29[7] (en adelante GT29) señaló que era un error partir del supuesto de que el tratamiento podía legitimarse a través del consentimiento de los trabajadores cuando el empresario debía tratar datos personales de estos. Es decir, cuando un empresario requiere del consentimiento de los trabajadores y existe un perjuicio real o potencial relevante en el caso de que el trabajador no dé su consentimiento, dicho consentimiento no será válido en base a que éste no habrá sido otorgado de forma libre. El GT29 indicaba que, en consecuencia, el consentimiento no se debía otorgar por parte de los trabajadores, sino que se debía buscar una base jurídica distinta a fin de no vulnerar sus derechos y que el consentimiento pudiera considerarse válido. Es decir, solamente el trabajador podrá otorgar consentimiento cuando éste pueda darse de forma libre y se tenga la posibilidad de rectificar posteriormente sin tener que asumir ningún tipo de perjuicio, según indicó el GT29 en su Dictamen 15/2011. Bajo estas premisas, el propio Grupo emitió un nuevo Dictamen, 2/2017, en el que insistía en este hecho justificándolo en que la relación entre empresario y trabajador podría ser conflictiva. A modo de ejemplo, difícilmente un trabajador otorgará consentimiento libre al empleador cuando éste se lo requiera para la instalación de sistemas de video-vigilancia y grabación de sonidos. Ante estos supuestos, el GT29 considera que el consentimiento no es una condición de legitimación válida cuando existe una relación laboral ya que la posición de subordinación del trabajador frente al empresario puede provocar que su manifestación no sea libre.

2.2.1.2. El contrato de trabajo como base jurídica del consentimiento.

El Reglamento europeo considera que el tratamiento será lícito cuando sea necesario para la ejecución de un contrato en el que el interesado forma parte de él. En ese sentido, el considerando 44 del RGPD contempla que *"…el tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato…"*.

[7] El GT29 es un órgano de carácter consultivo independiente creado por la Directiva 95/46/CE formado por representantes de los Estados miembros cuyo objetivo es estudiar, asesorar y emitir dictámenes sobre la aplicación de medidas de los Estados miembros en materia de protección de datos. El GT29 se regula en el artículo 29 y siguientes de la mencionada Directiva y debe su nombre al artículo de ésta.

Asimismo, el TC en su Sentencia 39/2016 FJ (3) expuso que *"…en el ámbito laboral, el consentimiento del trabajador pasa, (…) como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes…".*

Por otro lado, se podrán obtener datos sin que exista consentimiento como por ejemplo a la hora de formalizar el contrato de trabajo ya que hay datos que se tienen que proporcionar de forma obligatoria a fin de cumplir con los requisitos legales para la formalización contractual de la relación laboral. Sin embargo, esa dispensa es relativa ya que únicamente hace referencia a los datos necesarios para el mantenimiento y cumplimiento de la relación, es decir, a las obligaciones derivadas de las leyes y normas laborales como los convenios colectivos (DESDENTADO BONETE Y OTROS, 2011).

Finalmente, y en virtud del artículo 6.3 LOPD, los datos obtenidos por el empresario y que sirvan para la ejecución del contrato no deberán utilizarse para finalidades distintas a las del mantenimiento, desarrollo o control de la relación laboral.

2.2.1.3. Obligación legal aplicable al responsable del tratamiento.

El apartado c) del artículo 6.1 del RGPD reconoce como lícito el tratamiento de datos personales en cumplimiento de una obligación legal que se debe aplicar al responsable del tratamiento. Así, el considerando 45 del RGPD establece que en estos casos el tratamiento deberá tener una base en el Derecho comunitario o bien en el de los Estados miembros. Por tanto, en materia laboral el tratamiento de datos personales será lícito cuando se dé una obligación por el Real Decreto Legislativo 2/2015, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores[8] (en adelante, Estatuto de los trabajadores o ET), el Real Decreto Legislativo 8/2015, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social (en adelante, LGSS), la Ley 31/1995, de Prevención de Riesgos Laborales (en adelante, LPRL), la Ley 32/2006, reguladora de la subcontratación en el sector de la

[8] BOE núm. 255 (24-10-2015)

construcción, la Ley Orgánica 11/1985, de Libertad Sindical (en adelante, LOLS), la Ley 23/2015, ordenadora del Sistema de Inspección de Trabajo y Seguridad Social y la Ley 36/2011, reguladora de la Jurisdicción Social (en adelante, LRJS).

2.2.1.4. El interés público o en el ejercicio de poderes públicos.

El apartado e) del artículo 6.1 del RGPD establece que *"…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…"*. En ese sentido, las Administraciones Públicas deberán justificar el tratamiento de datos personales mediante disposiciones legales. A modo de ejemplo, el GT29 manifestó en su Dictamen 2/2017 que estos casos eran habituales en el ámbito laboral ya que las empresas deben calcular los impuestos y los salarios de los trabajadores.

2.2.1.5. El interés legítimo del responsable del tratamiento.

En España el concepto de *"…interés legítimo…"* se interpreta de forma restringida y se aplica en situaciones limitadas. Se considerará que el tratamiento de datos personales por interés legítimo es lícito si dicho tratamiento es necesario para la consecución de unos objetivos siempre y cuando los intereses del responsable del tratamiento no prevalezcan sobre los derechos fundamentales del interesado que requiera de una mayor protección de datos personales. Por tanto, la aplicación de este supuesto por interés legítimo deberá analizarse de forma más minuciosa.

Según el GT29 considera que en el ámbito laboral este tipo de interés legítimo debe aplicarse cuando exista un interés real y actual que se corresponda con las actividades actuales de la empresa. Por tanto, según manifestó en el Dictamen 6/2014, cuando los intereses fueran vagos o simplemente especulativos, no configurarán una base jurídica suficiente para legitimar el tratamiento de datos personales.

El Dictamen 2/2017 del GT29 se centra en el interés legítimo como base legal del tratamiento de datos personales en el ámbito laboral. En él analiza la proporcionalidad del tratamiento de

los datos en relación con el interés legítimo que debe mantener el empleador. Según dicho Dictamen, el empleador deberá realizar una prueba de proporcionalidad para verificar que todos los datos obtenidos son necesarios para la finalidad del tratamiento. De igual forma, deberá valorar si el tratamiento de los datos conseguidos prevalece sobre los derechos fundamentales de los trabajadores en el puesto de trabajo y, en caso de que efectivamente sea lícito el tratamiento de los datos, deberá garantizar que la vulneración de derechos sea prácticamente inexistente (MERCADER UGUINA, 2019).

Por tanto, atendiendo a lo anterior, el responsable del tratamiento de datos personales, que en este caso sería el empleador, deberá asegurarse de que existe una finalidad o interés legítimo suficiente. El empleador deberá utilizar un sistema para el tratamiento que sea proporcional a las necesidades del negocio procurando que genere la menor invasión posible para el trabajador.

2.2.2. Las garantías positivas y negativas en la protección de datos

2.2.2.1. Garantías positivas.

Las garantías positivas son aquellas que se contemplan para realizar determinadas conductas.

En primer lugar, el **principio de transparencia** consiste, según el artículo 12 del RGPD y el artículo 1 de la LOPD, en que toda información y comunicación relacionada con el tratamiento de datos sea de fácil acceso y comprensión. Este principio se refiere principalmente a la información de los interesados sobre quién es el responsable del tratamiento y qué fines tiene el mismo. Asimismo, se refiere al resto de información aportada para garantizar que el tratamiento de los datos personales será transparente en relación con las personas físicas afectadas (ORELLANA CANO, 2019).

Tal y como se ha indicado en puntos anteriores, el Reglamento prevé que sean los Estados miembros los que regulen la protección de datos en el ámbito laboral mediante disposiciones legales o convenios colectivos estableciendo así normas más específicas que garanticen los derechos y libertades relativos a la protección de datos de los trabajadores. Y añade que se deberán garantizar los derechos fundamentales *"…prestando especial atención a la transparencia del tratamiento…"* (RGPD art 88.2).

En consecuencia, el responsable del tratamiento deberá tomar las medidas oportunas para que el interesado pueda acceder a toda la información y comunicación relativa al tratamiento de forma concisa, transparente, inteligible y de fácil acceso según expone el RGPD 12.1. En ese sentido, el responsable del tratamiento podrá solicitar información adicional para poder verificar que el afectado es efectivamente el interesado, en este caso un trabajador, afectado por el tratamiento (MERCADER UGUINA, 2019).

El interesado deberá recibir la información solicitada por escrito o por otros medios y en ningún caso cabe la posibilidad de que el responsable del tratamiento tenga disponible la información en algún sitio, sino que se debe comunicar directamente a la persona interesada. El interesado podrá optar por presentar la solicitud por medios electrónicos o no electrónicos, sin perjuicio de que el empresario tendrá la obligación de facilitar que el interesado, en este caso el trabajador, pueda presentarla por medios electrónicos (GOÑISEIN, 2018). Asimismo, el responsable del tratamiento deberá facilitar la información sobre las actuaciones que hubiera llevado a cabo cuando existiera una solicitud por parte del interesado en el plazo de un mes desde la notificación de dicha solicitud. Ahora bien, existe la posibilidad de prorrogar dicho plazo en dos meses más (RGPD Art. 12.3) siempre y cuando el responsable informe con antelación al interesado exponiendo los motivos de la demora. Este tipo de comunicaciones se deberán realizar a título gratuito excepto cuando las solicitudes no tengan ningún fundamento.

En caso de que el responsable del tratamiento no tramitara la solicitud recibida, deberá informar al interesado de forma inmediata o bien en el plazo máximo de un mes desde la recepción de la solicitud sobre los motivos de su no actuación y, en segundo lugar, de la posibilidad de presentar una reclamación ante la autoridad de control (RGPD 12.4). Ahora bien, existen dos supuestos en los que el responsable del tratamiento podrá tomar la decisión de no actuar ante la recepción de una solicitud. Esos casos se darían cuando tenga dudas sobre la identidad de la persona física solicitante y cuando las solicitudes sean manifiestamente infundadas o excesivas (RGPD Art. 12.5). Será en este segundo caso en el que el responsable deberá demostrar el carácter manifiestamente infundado y excesivo de las solicitudes (GOÑISEIN, 2018).

En segundo lugar, el **derecho de información** (RGPD Arts. 12, 13 y 14; LOPD art. 11) se debe garantizar con motivo de lo expuesto por el TC en su sentencia 292/2000 FJ (7, 8 y 9). Según dicha sentencia, las personas deben tener garantizado el poder de control sobre sus datos personales, pero para tener el poder de disposición sobre sus datos deberá ser conocedor de cuáles son los que se poseen por terceros, quiénes los poseen y con qué fin.

La información que se debe facilitar al interesado es aquella que consta en el RGPD art. 13 y que dice lo siguiente: la identidad y los datos de contacto del responsable y, su caso, de su representante; los datos de contacto del delegado de protección de datos (en adelante, DPD), en su caso; los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; los intereses legítimos del responsable o de un tercero cuando el tratamiento se base en el art. 6.1.f); los destinatarios o las categorías de los destinatarios de los datos personales; la intención del responsable de transferir los datos personales a un tercer país u organización internacional.

Asimismo, el responsable deberá informar al interesado del plazo en el que se conservarán sus datos personales, así como del derecho a solicitar al responsable del tratamiento el acceso a los datos personales, retirar el consentimiento, presentar una reclamación ante la autoridad competente y si se trata de una obligación o requisito legal que el interesado deba comunicar sus datos personales (BLÁZQUEZ AGUDO, 2018).

En el ámbito laboral, el responsable del tratamiento podría informar sobre estas materias en el contrato laboral que deba firmar la empresa y el trabajador. De tal manera, el trabajador podría darse por informado, aunque no debería considerarse que mediante el presente acto se manifestara el consentimiento. Simplemente tendría efectos informativos a fin de cumplir con la obligación del responsable de informar al interesado.

En tercer lugar, el **derecho de acceso** (RGPD art. 15; LOPD art. 13) es considerado por el TC en su sentencia 254/1993 como un pilar fundamental en los derechos del interesado del tratamiento de datos personales. En ese sentido se pronunció también el TJUE afirmando que *"…el derecho de acceso es indispensable, en particular, para permitir al interesado obtener, en su caso, del responsable del tratamiento de los datos, la rectificación, la supresión o el bloque*

de esos datos y, en consecuencia, ejercer el derecho que se contempla en el artículo 12, letra b), de dicha Directiva…"[9].

El derecho de acceso consiste en la potestad del interesado de obtener confirmación por parte del responsable del tratamiento de si están tratando datos personales propios y, en tal caso, poder conocer cuáles son esos datos que particularmente son: los fines del tratamiento; las categorías de datos personales tratados; los destinatarios; el plazo de conservación; el derecho a solicitar la rectificación o supresión de datos personales; el derecho a presentar una reclamación; el origen de la información obtenida cuando ésta no provenga directamente del propio interesado; la existencia de decisiones automatizadas.

Para que se entienda que el derecho de acceso se ha otorgado, el responsable debe facilitar al afectado un sistema de acceso remoto, seguro y directo. Sin embargo, el afectado puede elegir un medio distinto al que se le ofrece. Ahora bien, cuando este medio distinto suponga un coste desproporcionado, la solicitud se considerará excesiva y, por tanto, deberá asumir el afectado los costes de su elección (MERCADER UGUINA, 2019).

El afectado tendrá derecho a obtener una copia de los datos personales objeto del tratamiento sin que afecte negativamente a los derechos y libertades de terceras personas (RGPD art. 15.4). En ese sentido se pronunció la Audiencia Nacional (en adelante AN) en el FJ 2 de su sentencia de 19 de marzo de 2014 indicando que el derecho de acceso *"…tan solo alcanza a los datos personales del titular de aquel derecho o a los de aquellas personas cuya representación ostentase, sin que quepa aceptar que incluye el derecho a acceder a datos de carácter personal de otras personas, pues ello comportaría la vulneración de su derecho fundamental a la protección de datos, consagrado en el artículo 18.4 de la Constitución…"*[10].

El **derecho a la portabilidad** (RGPD art. 20, LOPD art. 17) consiste en el derecho del afectado a transmitir de forma directa los datos personales de un responsable del tratamiento a otro. Para su cumplimiento, el Reglamento establece que los datos personales se deberán facilitar de forma estructurada, en una forma de uso común y de lectura mecánica (GOÑISEIN, 2018).

[9] TJUE 20-12-17, FJ (56 y 57), asunto Peter Nowak, C-434/16
[10] Sentencia de la Audiencia Nacional, sala contencioso-administrativo, de 19 de marzo de 2014, Rec. 176/2012.

El responsable del tratamiento deberá facilitar al interesado la información relativa a sus actuaciones en el plazo máximo de un mes desde la recepción de la solicitud que podría ampliarse hasta tres meses cuando concurran causas complejas y se le comunique al interesado de este hecho.

2.2.2.2. Garantías negativas.

El **derecho de rectificación** (RGPD art. 16; LOPD art. 14) consiste en que el afectado podrá corregir los errores existentes o modificar los datos que sean inexactos o incompletos, así como cuando sean inadecuados o excesivos. Este derecho está íntimamente ligado al derecho de acceso ya que este último tiene precisamente como finalidad que el interesado pueda corregir o modificar los datos obtenidos por el responsable del tratamiento.

El responsable del tratamiento estará obligado a dar una respuesta a las solicitudes de los interesados sin dilación y, en caso de que no quisiera atenderlas, debería indicar los motivos.

Por otro lado, el **derecho de supresión** (RGPD art. 17; LOPD art. 15) es definido como la cancelación de los datos personales que había obtenido el responsable del tratamiento. El Reglamento determina en qué situaciones se podrá proceder a la supresión de los datos personales cuando los datos del interesado ya no sean necesarios en relación con los fines del tratamiento, cuando el interesado retire su consentimiento, cuando el interesado se oponga al tratamiento, cuando los datos hubiesen sido tratados de forma ilícita, cuando los datos personales deban ser suprimidos en cumplimiento de alguna disposición legal, cuando los datos personales se hubiesen obtenido en relación con la oferta de servicios de la sociedad de la información del RGPD art. 8.1. El derecho de supresión también es conocido como derecho al olvido en los buscadores de internet.

Asimismo, existen diversas disposiciones particulares en relación con el derecho de supresión entre las que encontramos aquella relativas a los sistemas de video-vigilancia (FERRER SERRANO, 2019). La LOPD art. 22.3 establece que *"…los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de las personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad*

competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación…". Este precepto está íntimamente vinculado al artículo 89 de la misma Ley el cual hace referencia al derecho a la intimidad frente al uso de dispositivos de video-vigilancia y de grabación de sonidos en el lugar de trabajo.

El **derecho de bloqueo** (LOPD art. 32) consiste en que el responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión. Es decir, se deberán identificar y reservar los datos correspondientes adoptando una serie de medidas que impidan su tratamiento, así como su visualización. Este bloqueo quedará exceptuado cuando los datos tuvieran que ser facilitados a jueces y tribunales, Ministerio Fiscal o a las Administraciones Públicas competentes. En el momento que las actuaciones quedaran prescritas, el responsable del tratamiento de los datos personales deberá destruirlos.

Asimismo, el afectado o interesado tiene el **derecho de limitación del tratamiento** (RGPD art. 18; LOPD art. 16) que consiste en el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro (RGPD art. 4.3).

El interesad podrá obtener del responsable la limitación del tratamiento de datos cuando se cumpla alguna de las siguientes condiciones: que el interesado impugne la exactitud de los datos personales; que sea un tratamiento ilícito y el interesado no quiera la supresión de los datos; que el interesado necesite el mantenimiento de los datos personales para la defensa de reclamaciones; que el interesado se hubiera opuesto al tratamiento en virtud del RGPD art. 21.1.

El responsable del tratamiento estará obligado a responder a las solicitudes del interesado sin dilación con el plazo máximo de un mes y, en caso de que no fuera a atender las solicitudes deberás exponer los motivos (RGPD art. 12.4).

Finalmente, el **derecho de oposición** (RGPD art. 21 y 22; LOPD art. 18) consiste en el interesado podrá oponerse en cualquier momento a que datos personales que le afecten sean objeto de un tratamiento basado en el RGPD art. 6.1.e) y f). Sin embargo, no será podrá ejercer el derecho de oposición en los casos expuestos en los artículos 6.1.a), b) y c) del Reglamento.

Ante el derecho de oposición, el responsable del tratamiento deberá de dejar de tratar los datos personales a no ser que se acreditaran motivos legítimos imperiosos para su

tratamiento siempre y cuando prevalecieran sobre los derechos fundamentales del interesado (RGPD 21.1).

2.2.3. Límites de los derechos del interesado o afectado.

El RGPD art. 23 establece que el Derecho comunitario o el de los Estados miembros podrá limitar el alcance de las obligaciones y de los derechos reconocidos en el Reglamento. Particularmente, estos límites harán referencia a los derechos reconocidos en los artículos del 12 al 22 y el artículo 34, así como en el artículo 5 siempre y cuando los derechos y obligaciones sean los contemplados en los artículos 12 a 22. Ahora bien, estas limitaciones deberán respetar los derechos fundamentales teniendo que ser medidas necesarias y proporcionadas en un Estado democrático para salvaguardar la seguridad del Estado; la defensa; la seguridad pública; la prevención, investigación, detección o enjuiciamiento de infracciones penales; objetivos importantes de interés público; la protección de la independencia judicial; la prevención, investigación, detección y enjuiciamiento de infracciones relativas a normas deontológicas; supervisión e inspección en el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); la protección del interesado o de los derechos y libertades de terceras personas; la ejecución de demandas civiles (PIÑAR MAÑAS, 2019).

Finalmente, en el RGPD 23.2 determina que las medidas legislativas indicadas anteriormente contendrán disposiciones específicas sobre la finalidad del tratamiento o de sus categorías; las categorías de datos personales; el alcance de las limitaciones establecidas; las garantías para evitar accesos o transferencias ilícitas; la determinación del responsable de sus categorías; los plazos de conservación y las garantías aplicables; los riesgos para los derechos y libertades de los interesados; el derecho de los interesados a ser informados sobre la limitación.

2.3. El Responsable del tratamiento de la protección de datos

2.3.1. La empresa.

El RGPD art. 4.7 determina que el *"…responsable del tratamiento o responsable es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento*…".

El GT29 expuso en su Dictamen 1/2010 de 16 de febrero de 2010 la interpretación que hacía sobre el concepto responsable del tratamiento en virtud de la Directiva consistía en tres elementos que son los siguientes: a) en primer lugar, el aspecto personal ya que hacía referencia a la persona física o jurídica, autoridad pública o servicio o cualquier otro organismo; b) La posibilidad de que de que el tratamiento de datos se realizara de forma exclusiva por parte de un responsable o bien de forma conjunta. En ese sentido, el RGPD art. 26 contempla la existencia del corresponsable del tratamiento; c) Las funciones que debe realizar el responsable en relación con la determinación de los fines y de los medios del tratamiento de los datos personales.

En relación con la corresponsabilidad del tratamiento, el Reglamento dispone que serán los corresponsables los que deberán determinar de forma transparente y de mutuo acuerdo las responsabilidades respecto al tratamiento de datos personales. En el acuerdo alcanzar entre los corresponsables deberán constar las funciones y las relaciones respectivas con los interesados.

Expuesto lo anterior, se debe indicar que en el ámbito laboral se considerará responsable del tratamiento al empresario o empresa, si bien es cierto que podrán participar otros sujetos como responsables como por ejemplo los servicios de prevención. Según el RGPD art. 4.18, por empresa se debe entender aquella *"…persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica*…".

Por otro lado, no se debe obviar la existencia de los grupos de empresa, los cuales según el RGPD art. 4.19 son aquellos grupos constituidos por una empresa que ejerce el control y sus empresas controladas. En ese sentido, el considerando 37 del Reglamento expone que *"…una*

empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas, grupo empresarial…".

Asimismo, el RGPD art. 88.2 establece que se deberán implantar medidas adecuadas para proteger la dignidad humana de los interesados, así como también sus derechos fundamentales. Para ello, continúa, se deberá tener una atención especial 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. Por tanto, el Reglamento reconoce la importancia que tienen los grupos de empresa y los conflictos que pueden generarse en relación con la protección de datos en el seno de un grupo empresarial.

Respecto a los grupos empresariales, el Informe AEPD 0494/2008 señaló que cada una de las empresas que conforman el grupo son personas jurídicas diferenciadas y que, por tanto, cada una de ellas son responsables del tratamiento de datos personales de sus empleados, independientemente de que exista una empresa matriz. En ese mismo sentido se pronunció el Tribunal Superior de Justicia de Madrid afirmando que *"…si la recurrente ha preferido constituir dos sociedades y trabajar con ellas de manera independiente, beneficiándose así del mantenimiento de dos personas jurídicas distintas, no puede, al mismo tiempo, pretender justificar el conocimiento por parte de la matriz de los datos que le constan a la filial por las operaciones que esta última ha intervenido pues ello supone olvidarse de que se trata de personas jurídicas distintas…"*[11]. Es decir, el Tribunal respeta que existan dos personas jurídicas diferenciadas y que entre ellas conformen un grupo de empresas porque así lo prevé también el Derecho Mercantil. Ahora bien, lo que viene a defender el Tribunal es que una persona que contrate una de estas empresas no puede verse afectado por la estructura empresarial que las sociedades hubieran elegido (MERCADER UGUINA, 2019)).

A mayor abundamiento, si se diera el caso de que una de las empresas que forma parte del grupo tuviera acceso a los datos de cualquiera de las otras, se estaría ante un caso de

[11] TSJ Madrid 16-10-00, Rec. 1132/97

comunicación o cesión de datos que requeriría alguna de las bases de legitimación del RGPD art. 6.

En cuanto a las obligaciones del responsable del tratamiento de datos personales, el RGPD art. 30 establece que deberá llevar un registro de las actividades del tratamiento. Dicho registro deberá contener la información específica requerida. De igual forma, se llevará un registro con todas las categorías de actividades de tratamiento efectuadas por el responsable. Este registro deberá constar por escrito, en formato electrónico y se deberá poner a disposición de la autoridad de control competente.

Sin embargo, quedarán exceptuadas aquellas organizaciones o empresas que empleen a menos de 250 trabajadores. Estarán exentos a no ser que el tratamiento pueda suponer un riesgo para lo derechos fundamentales de los interesados; no sea ocasional; incluya categorías especiales de datos personales; incluya datos personales relativos a condenas e infracciones penales.

Asimismo, el Responsable deberá asegurarse de que los datos obtenidos fueran adecuados y veraces, así como se hubieren obtenido de forma lícita y el tratamiento fuera proporcional a la finalidad prevista. Deberá garantizar el cumplimiento del secreto y seguridad y deberá informar a los interesados de la recogida de los datos. Para obtener dichos datos, deberá obtener primeramente el consentimiento para el tratamiento de los mismos pudiendo los interesados posteriormente ejercer sus derechos de oposición, acceso, rectificación y cancelación sin que el responsable pudiera oponerse a no ser que se trate de una solicitud abusiva. Finalmente, el Responsable deberá asegurar que de las relaciones con terceros se cumpla en todo momento lo previsto en el RGPD y en la LOPD, así como cumplir la normativa sectorial de aplicación según el caso (PRECIADO DOMÈNECH, 2019).

2.3.2. El encargado del tratamiento.

El RGPD art. 4.8 define al encargado del tratamiento como aquella persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. La afirmación *"…por cuenta del responsable del tratamiento…"*

implica que entre el responsable y el encargado existe una relación jurídica que los vincula delimitando así el ámbito de actuación de cada uno de ellos.

En el ámbito laboral, los encargados del tratamiento de datos personales podrían ser todas aquellas personas físicas o jurídicas que realicen funciones relacionadas con la empresa como por ejemplo las gestorías que hacen las nóminas, las empresas de prevención de riesgos laborales o los servicios jurídicos externos que tenga contratados la empresa. Es decir, el encargado del tratamiento es aquella persona física o jurídica que ha sido contratada por la empresa responsable del tratamiento de datos personales a fin de que realice una tarea concreta vinculada a la misma. En el ámbito laboral es muy habitual que existan encargos de tratamiento en la gestión del personal laboral y se producen cuando la empresa decide descentralizar actividades a través de personas externas. Ahora bien, las empresas podrían evitar la externalización de servicios y, por tanto, no asignar un encargado del tratamiento, contratando a personal que realice de forma interna dicha actividad.

No obstante, el encargado actúa por cuenta del responsable y, por tanto, la relación jurídica entre ambas partes no es jerárquica como la existente entre empresario y trabajador, sino que se trata de una delegación de funciones entre personas jurídicamente diferenciadas.

Según el Dictamen 1/2010 GT29, para poder ser encargado del tratamiento se debía tratar en primer lugar de una entidad independiente del responsable y, en segundo lugar, que se trataran los datos por cuenta de este.

El encargado del tratamiento de datos personales estará legitimado a ejercer como tal siempre y cuando se le haya conferido un mandato por parte del responsable. En ese sentido, el encargado únicamente tendrá acceso a los datos personales que se le hubiesen proporcionado en el momento en que lo encargase el responsable. Hay que tener en cuenta que el encargado también podría disponer de personal propio el cual también tendría acceso a dichos datos con la finalidad de cumplir con el encargo efectuado. Asimismo, no hay que olvidar que el encargado presta unos servicios por cuenta del responsable del tratamiento, lo que implica que solamente podrá tratar dichos datos bajo un sometimiento estricto a las indicaciones del responsable. En caso contrario, es decir, en caso de que el encargado decidiera cómo realizar el tratamiento obviando al responsable, la AEPD, según ha expuesto

en diversos informes, el Encargado pasaría a ser responsable en vez de encargado lo que implicaría la asunción de las responsabilidades correspondientes[12].

Por todo ello, el encargo efectuado por el responsable en favor del encargado deberá constar en un documento escrito en el que se haga constar expresamente el deber del encargado de tratar los datos personas según las instrucciones dadas por el responsable del tratamiento. De tal forma, se deberá hacer constar el compromiso de no utilizar dichos datos con finalidades distintas a las pactadas. En dicho documento o contrato que vincule a las dos partes deberá constar también el objeto, la duración, la naturaleza y la finalidad del tratamiento, incluyendo el tipo de datos personales y las categorías de interesados, y las obligaciones y derecho del responsable.

Asimismo, el Encargado del tratamiento no debe recurrir a otro encargado sin la autorización del responsable del tratamiento. Dicha autorización debe ser por escrito.

Por otro lado, el contrato deberá contemplar que el encargado trate los datos personales siguiendo únicamente las instrucciones documentadas del responsable. En ese sentido, el encargado deberá obtener instrucciones específicas sobre las transferencias de datos personales a un tercer país o una organización internacional, excepto si estuviera obligado en virtud del Derecho comunitario o de los Estados miembros. En ese caso, el encargado deberá informar al responsable a no ser que el Derecho no lo permita por motivos de interés público.

El encargado deberá garantizar que las personas autorizadas a tratar los datos de carácter personal se hubieran comprometido a respetar la confidencialidad o bien se encontraran sujetas a una obligación de confidencialidad (TRONCOSO REIGADA, 2010). Asimismo, el encargado deberá tomar las medidas necesarias para garantizar la seguridad de los datos personales tratados y deberá respetar las condiciones para recurrir a otro encargado del tratamiento.

El encargado deberá asistir al responsable mediante medidas técnicas y organizativas idóneas, con la finalidad de que este pueda responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados. Asimismo, deberá ayudar o asistir al responsable

[12] AEPD Informe 0333/2012; 0227/2010; 0173/2009.

a garantizar el cumplimiento de las obligaciones sobre la seguridad en el tratamiento de los datos personales.

Cuando finalice la relación contractual, el encargado deberá eliminar o devolver según se lo requiera el responsable los datos personas que hubiera utilizado para su tratamiento. Ante esta obligación, también deberá suprimir o devolver las copias de seguridad que hubiera realizado, a no ser que el Derecho comunitario o de los Estado miembros exigiera su conservación.

2.3.3. El delegado de protección de datos

El delegado de protección de datos es una figura introducida por el RGPD y tiene como funciones principales la supervisión de una forma independiente la aplicación de la normativa de protección de datos. El RGPD art. 37.1 establece que las empresas estarán obligadas a designar un delegado de protección de datos siempre que las actividades principales del responsable consistan en operaciones de tratamiento que requieran de una observación habitual y sistemática de interesados a gran escala. Asimismo, se deberá designar DPD cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especial de datos personales. No hay que olvidar, que también será obligatoria su designación cuando el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales cuando actúe en el ejercicio de su función judicial.

En el caso español, la LOPD art. 34 expone una serie de supuestos en los que se deberá proceder a la designación del delegado de forma obligatoria, dejando que en el resto de casos la decisión de la designación sea plenamente voluntaria. Es importante remarcar que por ese motivo el DPD no tiene responsabilidad a título personal, ya que en caso de cometerse infracciones en materia de protección de datos será la empresa quien deba asumir dicha responsabilidad (RECIO GAYO, 2019)

El DPD deberá informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen de dicho tratamiento de las obligaciones que les corresponden en relación con el Reglamento europeo y la LOPD en el caso de España.

Asimismo, deberá supervisar el cumplimiento de lo dispuesto en la normativa comunitaria y la de los Estados miembros en relación con la protección de datos y de la política de actuación del responsable o encargado del tratamiento.

En virtud del RGPD art. 35, el delegado deberá supervisar la aplicación de la evaluación de impacto relativa a la protección de datos y, en su caso, deberá asesorar al responsable o encargado para un mayor cumplimiento de la normativa.

Finalmente, el delegado deberá cooperar con la autoridad de control siendo, a su vez, la persona de referencia para cuestiones relativas al tratamiento de datos personales teniendo que intervenir también en caso de reclamación ante dichas autoridades competentes.

La normativa laboral no establece los derechos y obligaciones que ostentan los trabajadores en relación con la materia de protección de datos personales. Es por ello que se deberá estar lo que dispone el RGPD y la LOPD, así como también a la proliferación de nuevos códigos éticos para el delegado de protección de datos siempre y cuando fueran autorizados por la AEPD.

Tal y como se ha indicado anteriormente, el delegado de protección de datos actuará con independencia sin recibir instrucciones de ningún tipo por parte del responsable o encargado del tratamiento. Es decir, en caso de que el delegado fuera empleado del responsable o del encargado, en ningún caso podrá recibir instrucciones que vulneren su independencia en el ejercicio de sus funciones tal y como se contempla en el RGPD considerando 97.

Atendiendo a lo anterior, el delegado de protección de datos deberá cumplir las órdenes de su superior jerárquico en virtud del ET art. 5.c) siempre y cuando las funciones no tuvieran vinculación con el ejercicio directo de delegado de protección de datos, a no ser que supusiera un conflicto de intereses para el delegado. Es decir, las funciones como delegado de protección de datos se ejercerán sin la intromisión del superior jerárquico en virtud de la independencia del cargo, pero, a su vez, será un subordinado para todas aquellas funciones que supusieran una vulneración de dicha independencia en el ejercicio de la protección de datos.

Por tanto, el delegado de protección de datos no podrá ser destituido ni sancionado por el ejercicio de sus funciones según el RGPD art. 38.3. Sin embargo, tal y como consta en las *Directrices sobre los delegados de protección de datos (WP 243)* del GT29, la inmunidad del

delegado de protección de datos no significa que no pueda ser despedido por causas objetivas que podrían surgir por una mala realización de sus tareas o como incumplimiento de sus obligaciones. En ese sentido, la LOPD art. 36.2 establece que el delegado de protección de datos podría ser despedido cuando incurra en dolo o negligencia grave.

Finalmente, y no por ello menos importante, el delegado de protección de datos no será personalmente responsable cuando concurran causas de incumplimiento de la normativa ya que quienes deben responder frente a actos ilícitos en el tratamiento de protección de datos son los responsables o, en su caso, los encargados. El motivo es claro: el responsable y el encargado son las personas que deben garantizar el cumplimiento de la normativa estableciendo mecanismos idóneos para ello (RGPD art. 24.1).

2.4. Los sistemas de video-vigilancia y el control de la empresa.

2.4.1. La grabación de imagen y sonido como dato personal.

Según la AEPD la grabación de imágenes y de sonidos de una persona, independientemente de que sea o no trabajador de la empresa, es un dato personal[13]. En ese sentido, la Guía para el Ciudadano define el dato de carácter personal como *toda información sobre una persona física identificada o identificable ("el interesado")*. Y la definición continúa indicando que se entenderá como persona física identificable aquella que pueda ser reconocida de forma directa o indirecta mediante un identificador que podría ser, por ejemplo, un nombre.

Asimismo, el GT29 ha indicado que los datos constituidos por imágenes y sonidos deben ser reconocidos como de carácter personal a pesar de que dichas imágenes se utilicen en el marco de un circuito cerrado y no se asocien a los datos personales del interesado[14].

[13] AEPD Resolución R/00035/2006 27-2-06.
[14] AEPD Informe 0533/2006.

2.4.2. La proporcionalidad del sistema de video-vigilancia.

La AEPD ha indicado que *"…en ningún caso el empresario pueda tratar datos personales que no sean directamente relevantes en el ámbito de la relación laboral, como el comportamiento o las características personales de los trabajadores o los contactos internos con otros trabajadores o externos del trabajador…"*[15].

En ese sentido, el principio de proporcionalidad juega un papel muy importante a la hora de valorar si el sistema de video-vigilancia está justificado o no en el ámbito laboral. El motivo de por qué se debe analizar la proporcionalidad de la medida reside en el serio peligro que puede suponer la instalación de este tipo de sistemas y se vulneren derechos fundamentales de los trabajadores generando así situaciones completamente abusivas. La AEPD ha afirmado que el principio de proporcionalidad evita la vigilancia omnipresente impidiendo la vulnerabilidad del trabajador[16]. Por tanto, es evidente que resulta completamente desproporcionado el seguimiento continuado de las actividades de los trabajadores (MERCADER UGUINA, 2019).

A modo de ejemplo, resulta paradigmática la instalación de una webcam en la redacción de un periódico a la cual podía acceder cualquier persona pudiendo observar cómo prestaban servicios los trabajadores durante las 24 horas del día. En ese caso, la Audiencia Nacional consideró que se había vulnerado la normativa de protección de datos ya que excluía la existencia de un consentimiento tácito ya que el hecho de que *"…los trabajadores haya soportado la captación de imágenes con una cámara situada en la redacción o hayan permanecido inactivos ante esta iniciativa de la empresa no permite afirmar que estén conformes con ella ni que hayan dado su consentimiento cuando ni siquiera consta que hubiesen sido previamente informados sobre las características y el alcance del tratamiento de datos que iba a realizarse…"*[17].

Más conflictivo es el caso en el que se instala un sistema de video-vigilancia en un domicilio donde presta servicios una empleada del hogar. El RGPD art. 2.2.c) contempla la excepción doméstica por la que el Reglamento no es de aplicación a los tratamientos efectuados por una

[15] AEPD Informe 0475/2014.
[16] AEPD Informe 0495/2009.
[17] AN cont-adm 24-1-03, EDJ 249138.

persona física en el ejercicio de actividades domésticas o personales. Asimismo, atendiendo al considerando 18 del Reglamento, dichas actividades domésticas o personales no deberían suponer una actividad profesional o comercial. Por tanto, en el caso de las empleadas del hogar la captación de imágenes estará condicionada al cumplimiento del RGPD ya que la actividad estará amparada en el ET art. 20.3 (RODRÍGUEZ ESCANCIANO, 2019).

2.4.3. Sobre la licitud del tratamiento.

El tratamiento de datos recogidos por el sistema de video-vigilancia del empleador se justifica en virtud de la LOPD art. 22.8 y 89. Asimismo, no hay que olvidar que el ET art. 20.3 establece que *"…el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad…"*.

No obstante, hay que tener en cuenta que tal y como se desprende de la LOPD no se admitirá que el sistema de video-vigilancia se instale en lugar destinados al descanso o esparcimiento de los trabajadores (GONZÁLEZ GONZÁLEZ, 2019). De igual forma, la AEPD ha recomendado que las cámaras que puedan orientarse deberán utilizar máscaras de privacidad con la finalidad de evitar captar imágenes de la vía pública o espacio ajeno al de la empresa.

2.4.4. Derecho de información de los trabajadores.

Según establece el artículo 89.2 LOPD, los empleadores deberán informar a los trabajadores y, en su caso, a los representantes de los trabajadores previamente y de forma expresa, clara y concisa sobre la aplicación del sistema de video-vigilancia. En ese sentido, la AEPD ha recomendado en innumerables ocasiones que en ningún caso se deberá informar previamente a los trabajadores a través de llamadas a teléfonos privados, como tampoco a direcciones particulares.

Sin embargo, hay que tener en cuenta cómo y cuándo se puede entender que los trabajadores han sido informados correctamente según indica el reglamento. Así, la AEPD ha indicado que

los carteles informativos conforme en el centro de trabajo se ha instalado un sistema de video-vigilancia deben encontrarse en un lugar suficientemente visible, independientemente de que se trate de un lugar abierto o cerrado (VALVERDE ASENCIO, 2013). Es decir, no existe la obligación de colocar el cartel informativo justo debajo de la cámara de video-vigilancia, sino que simplemente deberá constar en un lugar en el que los trabajadores puedan visualizarlo sin problemas. Asimismo, la AEPD también se ha pronunciado sobre la dimensión mínima indicando que no existe ningún criterio en relación con dicho aspecto. No obstante, ha considerado que el tamaño del cartel informativo instalado por el responsable del tratamiento debe ser lo suficientemente grande para que pueda ser identificado.

Atendiendo a lo anterior, los trabajadores o empleados públicos que hubieran cometido algún acto ilícito y hubiese sido captado por un sistema de video-vigilancia, se considerarán informados cuando existiera al menos un cartel informativo en un lugar visible en el que se pudiera identificar la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previsto en el RGPD art. 15 a 22. No obstante, cuando el uso de las imágenes obtenidas a través de sistemas de video-vigilancia sea para fines disciplinarios, es decir, para fines exclusivos de seguridad, o bien, cuando la instalación de cámaras con fines de control laboral sea temporal, y existan fundadas sospechas previas de incumplimientos laborales, se dará una excepción en cuanto a la obligación de informar (SERRANO OLIVARES, 2018).

El Tribunal Constitucional se ha pronunciado en cuanto al derecho del trabajador a ser informado sobre quién posee sus datos personales y con qué finalidad los utilizan (TC 29/2013). El supuesto examinado en la sentencia consistía en que un trabajador había sido sancionado disciplinariamente por infracciones relativas al cumplimiento de su horario laboral, en el que se habían constatado dichas infracciones gracias a la obtención de imágenes mediante sistemas de video-vigilancia. Según dicha sentencia, el responsable del tratamiento que hubiera instalado un sistema de video-vigilancia con la correspondiente autorización administrativa de la AEPD para el control de acceso de las personas en el centro de trabajo y se hubieren instalado distintivos anunciando la aplicación de dicho sistema, no podrá utilizar las imágenes captadas por dicho sistema de control si no se informó previamente al trabajador de que dicha captación podría servir para tomar medidas disciplinarias contra él. Es decir, el

sistema de video-vigilancia para la obtención de datos personales no tendrá amparo legal cuando tenga como fundamento el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados. En caso contrario, se estarían vulnerando derechos fundamentales en tanto que la información exigible al responsable del tratamiento de datos personales se les estarían negando a los trabajadores afectados.

Posteriormente, el Tribunal Constitucional matizó su doctrina con la Sentencia 39/2016. En el presente caso, una empresa despidió a una trabajadora por haberse apropiado de dinero de la caja del comercio en el que prestaba servicios habiendo obtenido la empresa las imágenes a través del sistema de video-vigilancia que había instalado como consecuencia de la detección de irregularidades en dicha caja. Uno de los hechos particulares de este caso es que la empresa no había informado previamente a la trabajadora de la instalación de dicho sistema. Sin embargo, el responsable del tratamiento sí que había instalado unos carteles informativos en un lugar visible conforme el centro estaba videovigilado. El TC consideró que no se había vulnerado el derecho fundamental (Const. Art. 18.4) de la trabajadora ya que el responsable del tratamiento había colocado distintivos informativos conforme se habían instalado cámaras de video-vigilancia, considerando que de tal forma ya se había cumplido con la obligación de información previa pese a que no se había indicado la finalidad exacta del control. En tal sentido, el TC consideró que la medida de vigilancia era proporcional a la situación de la empresa y, por tanto, concluyó que no se había vulnerado el derecho a la intimidad personal de la trabajadora. Así, el TC consideró en el FJ (5) de la sentencia que la medida era justificada porque existían sospechas previas de que había trabajadores que se apropiaban ilícitamente de dinero de la caja; que la medida era idónea para la finalidad de identificar si realmente eran los trabajadores los que cometían dichas irregularidades y poder, posteriormente, sancionar disciplinariamente a los responsables; que la medida era necesaria en tanto que las imágenes obtenidas constituían una prueba; y, finalmente, que la medida era equilibrada ya que únicamente se centró en la zona de la caja.

El Tribunal Europeo de Derechos Humanos (en adelante, TEDH) se pronunció al respecto en su Sentencia de 8 de enero de 2018 en el Caso López Ribalda y Otros Asuntos 1874/13 y 8567/13 con la particularidad que en este caso el sistema de video-vigilancia se encontraba oculto. De la misma forma que en el anterior supuesto, la empresa decidió instalar cámaras

de video-vigilancia porque existían fundadas sospechas de que los trabajadores se apropiaban dinero de la caja. Sin embargo, la empresa únicamente informó a los trabajadores de la existencia de unas cámaras de video-vigilancia que eran visibles y que enfocaban a las salidas del centro de trabajo, pero no informó de las que se encontraban ocultas y que enfocaban a la zona de las cajas. Ante tal situación, el TEDH consideró, según consta en FJ (69), que se habían vulnerado los derechos fundamentales de los trabajadores ya que la video-vigilancia oculta de un trabajador en su puesto de trabajo es una injerencia en su derecho a la vida privada. Si bien es cierto que el tribunal consideró que el control de la empresa era idóneo porque existían sospechas de que se habían producido apropiaciones ilícitas de dinero de las cajas, consideró, por el contrario, que la medida no era proporcional. Dicha proporcionalidad se podría haber cumplido si se hubiera informado a los trabajadores de la existencia de dichas cámaras y, por tanto, hubiesen dejado de estar ocultas. Asimismo, hay que tener en cuenta que previamente a que los trabajadores fueran conocedores de la existencia de las grabaciones de video, los datos e imágenes obtenidos mediante dicho sistema de video-vigilancia habían sido tratados por personas que trabajan para el empresario, tales como el representante sindical o el representante legal de la empresa. Por todo ello, el Tribunal concluyó que se habían vulnerado derechos fundamentales de los trabajadores ya que no habían sido informados previamente de la existencia de dichas cámaras, así como tampoco de la finalidad de estas.

2.4.5. Los representantes de los trabajadores.

Según la LOPD Art. 89.1, los empleadores que quieran tratar imágenes obtenidas a través de sistemas de video-vigilancia deberán informar previamente a los representantes de los trabajadores siempre y cuando estos existan en la empresa. En ese sentido, el Informe 0006/2009 de la AEPD indicó que *"…en el ámbito laboral además de la información personalizada a los trabajadores de la que debe quedar la adecuada constancia, exige su comunicación a los representantes de los trabajadores…"*.

Asimismo, cuando una empresa decida instalar un sistema de video-vigilancia para realizar una un control del trabajo de sus empleados en virtud del ET Art. 20.3, deberá informar

previamente al comité de empresa cuando exista a fin de que este pueda valorar tal decisión. Así, el ET Art. 64.1 establece que el comité de empresa tendrá derecho a conocer o a ser informado de todas aquellas medidas que adopte la empresa y que puedan afectar a los trabajadores. A mayor abundamiento, el comité de empresa tendrá derecho a emitir un informe sobre las medidas adoptadas por la empresa vinculadas a *"…la implantación y revisión de sistemas de organización y control del trabajo, estudios de tiempos, establecimientos de sistemas de primas e incentivos y valoración de puestos de trabajo…"* (ET art. 64.5.j) (VALVERDE ASENCIO, 2013).

2.4.6. Los derechos de los trabajadores como interesados.

Tal y como se ha indicado en puntos anteriores, los derechos que los afectados, en este caso trabajadores, pueden ejercitar son el acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y oposición a decisiones individuales automatizadas (RGPD Art. 15 a 22). Sin embargo, en primer lugar, se deberá identificar ante quién se debe ejercitar cada uno de estos derechos ya que podrá ser ante el responsable o bien ante el encargado del tratamiento, siempre y cuando en este segundo caso lo hubieran acordado entre el responsable y el encargado.

Asimismo, según la Guía sobre el uso de videocámaras para seguridad y otras finalidades de la AEPD, el ejercicio de alguno de estos derechos debe ser limitado o matizado en el ámbito de la video-vigilancia. En ese sentido, el derecho de rectificación no sería posible ejercitarlo ya que las imágenes obtenidas son hechos objetivos y, por tanto, el derecho de rectificación en este caso se encuentra vacío de contenido, ya que las imágenes tomadas reflejan una realidad. Por otro lado, el derecho de portabilidad tampoco se puede ejercer por parte de los afectados ya que la legitimación no se basa ni en el consentimiento ni en la ejecución de un contrato. En relación con el derecho a la limitación del tratamiento, no se aplicaría la parte correspondiente a la cancelación cautelar vinculada al ejercicio de los derechos de rectificación y oposición.

No obstante, estas limitaciones no existen en relación con el derecho de acceso pese a que para poder acceder a las imágenes se requiera aportar una imagen actualizada que permita verificar al responsable del tratamiento que efectivamente dicho afectado es una de las

personas que consta en los registros de las imágenes (MERCADER UGUINA, 2019). Sin embargo, que un afectado acceda a las imágenes registradas implica que el responsable esté mostrando imágenes de otros afectado. Es por ello que puede facilitarse el acceso mediante un escrito certificado en el que se haga constar los datos que hubieren sido objeto de tratamiento, procurando así evitar la vulneración de derechos de terceras personas. Asimismo, los datos registrados como imágenes deben ser suprimidos en el plazo máximo de un mes desde su captación, excepto cuando existan imágenes que hubieren captado actos que atentaren contra la integridad de las personas, bienes o instalaciones, procurando en tal caso conservar las imágenes (LOPD Art. 22.3).

Finalmente, el derecho a la limitación del tratamiento se podrá aplicar cuando se solicite al responsable que se conserven las imágenes cuando el tratamiento de datos sea ilícito y el interesado se oponga a su supresión solicitando que se limite su uso. Asimismo, dicha limitación del tratamiento también se podrá solicitar al responsable cuando este ya no necesite los datos obtenidos para los fines previstos pero el interesado sí que los necesite para la formalización de la reclamación correspondiente en defensa de sus intereses.

2.5. La responsabilidad del responsable del tratamiento.

2.5.1. La indemnización por daños y perjuicios

Tal y como se desprende del RGPD Art. 82.2, en caso de que el tratamiento de datos no cumpliera con los dispuesto en la normativa de protección de datos, el responsable del tratamiento responderá de los daños y perjuicios que pudiera haber causado a los afectados. Ahora bien, de conformidad con el RGPD Art. 82.1 quien ostenta la legitimidad activa para iniciar cualquier acción en reclamación de daños y perjuicios será aquella persona que los hubiera sufrido.

Por otro lado, los sujetos responsables son aquellos previsto en el RGPD Art. 4.7. No obstante, hay que diferenciar la responsabilidad del responsable de la del encargado del tratamiento. En el caso del responsable del tratamiento parte de la doctrina considera que se aplica la regla de responsabilidad objetiva. En ese sentido, cuando se hubiera acreditado la infracción cuyas consecuencias hubiesen sido los daños y perjuicios del afectado, el responsable debería

indemnizar a este sin poder alegar el desconocimiento de la producción de dichos daños y perjuicios (TRUJILLO MACHUCA, 2020). Por tanto, en materia de responsabilidad civil se aplica un sistema de responsabilidad directa del responsable del tratamiento de datos personales. Ahora bien, otro sector de la doctrina considera que únicamente existirá el derecho a percibir la indemnización por los daños y perjuicios causados cuando estos se hubieren producido mediante dolo, culpa o negligencia por parte del responsable o encargado del tratamiento (MERCADER UGUINA, 2019). Es decir, tal y como determina el RGPD Art. 82.3, el responsable o encargado del tratamiento quedarán exentos de responsabilidad cuando se demuestre que no ha existido responsabilidad en el hecho que hubiera producido los daños y perjuicios correspondientes.

En el caso del encargado del tratamiento, únicamente responderá por los daños y perjuicios producidos cuando hubiera actuado de forma contraria a lo establecido en la normativa específica sobre el tratamiento de datos personales que efectúan los encargados o bien, en caso de que éste hubiera actuado al margen o de forma contraria a las instrucciones dadas por el responsable del tratamiento, según determina el RGPD art. 82.5.

Asimismo, hay que tener en cuenta que la responsabilidad del responsable y del encargado es solidaria entre ellos (RGPD 82.4). De esta manera, el Reglamento garantiza que se efectúe el abono de la indemnización por daños y perjuicios en favor del afectado o interesado. En ese sentido, cuando uno de los dos sujetos del tratamiento de datos personales abonara la totalidad de la indemnización al interesado, podrá repetir contra el otro a fin de que responda por la parte proporcional que le correspondiera (MERCADER UGUINA, 2019).

El propio Reglamento en su artículo 82.1, establece que serán indemnizables aquellos daños y perjuicios tanto materiales como inmateriales, es decir, no necesariamente deberán ser físicos o patrimoniales los daños y perjuicios, sino que se podrán valorar también los daños morales derivados del incumplimiento de la normativa en el tratamiento de los datos personales. Así, el RGPD considerando 146 establece que *"…el concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia…"*.

No obstante, hay que verificar que el daño causado fue efectivo y real, evaluable económicamente e individualizable con relación a una persona o grupo. Asimismo, hay que

tener en cuenta que del Reglamento no se extrae la conclusión de que por el simple hecho de haber cometido una infracción en materia de protección de datos se presuma la existencia de unos daños y perjuicios, sino que se debe acreditar la existencia de estos y la relación de causalidad entre la acción u omisión del responsable o encargado del tratamiento y los daños y perjuicios causados.

Asimismo, se puede dar el caso de que tanto el responsable como el encargado queden exentos de responsabilidad siempre y cuando demostraren que no fueron los causantes del daño, según el RGPD considerando 146 y del art. 82.3. En ese sentido, quedarán exentos cuando las causas del daño fueran externas al tratamiento de datos personales en tanto que se escapaban del control y supervisión de estos.

En cuanto al plazo para el ejercicio de la acción de responsabilidad civil, el RGPD no hace referencia a la prescripción y, por tanto, se debe acudir directamente al derecho interno de cada Estado miembro. Sin embargo, en el caso español no se contempla tampoco ningún plazo generando la duda de si se aplican los cinco años de prescripción al tratarse de responsabilidad contractual (CC art. 1964) o bien el plazo de cuatro años previsto en la LO 1/1982[18] art. 9.5 cuando la reclamación tenga su fundamento en la intromisión ilegítima del derecho al honor (TRUJILLO MACHUCA, 2020).

2.5.2. El Régimen sancionador

Según consta en la LOPD art. 70, los sujetos responsables que se ven afectados por el régimen sancionador establecido por el RGPD y la LOPD son los siguientes: a) Los responsables de los tratamientos; b) los encargados de los tratamientos; c) los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea; d) las entidades de certificación; e) Las entidades acreditadas de supervisión de los códigos de conducta a excepción del delegado de protección de datos.

[18] BOE núm. 115 (14-05-1982)

Asimismo, el considerando 11 del RGPD expone que la protección efectiva de los datos personales en la Unión Europea obliga a los Estados miembros a reconocer unos poderes que sirvan para supervisar y garantizar el cumplimiento de las normas relativas a la protección de datos mediante la aplicación de sanciones administrativas. En ese sentido, los considerandos 148 y 150 de Reglamento exponen que cuando se produzca una conducta contraria a la normativa de protección de datos, se deberán imponer sanciones de carácter administrativo, atendiendo cada caso de forma particular y valorando las circunstancias concretas de cada caso. No obstante, el considerando 152 del Reglamento va un paso más allá y expone que los Estados miembros deberán aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias, pudiendo llegar a ser estas sanciones de naturaleza penal según el Derecho de cada Estado miembro. Ahora bien, hay que indicar que se deberán aplicar las sanciones establecidas por los Estados miembros cuando estas no hubieren sido armonizadas previamente por el Reglamento.

El organismo responsable de imponer las sanciones administrativas es la autoridad de control que se hubiera creado en cada Estado miembros. En el caso de España, tal y como se ha indicado en innumerables ocasiones, la autoridad de control responsable de imponer las sanciones es la Agencia Española de Protección de Datos. Así, la AEPD deberá sancionar a los sujetos responsables del tratamiento de datos personales según se ha indicado anteriormente cuando cometan alguna infracción de forma que las sanciones sean individuales, efectivas, proporcionadas y disuasorias.

Para imponer las sanciones correspondientes, hay que tener en cuenta en primer lugar la graduación de las infracciones. Así, el RGPD arts. 83.4 y 5 y la LOPD art. 74 hacen referencia a las infracciones de carácter leve; el RGPD art. 83.4 y la LOPD art. 73 establecen las infracciones de carácter grave; y, finalmente, el RGPD art. 83.5 y la LOPD 72 estipulan las infracciones de carácter muy grave. Ahora bien, para determinar qué grado corresponde a la infracción que se hubiera cometido hay que valorar previamente los criterios de graduación establecidos en el RGPD 83.2 y la LOPD art. 76.

Finalmente, las sanciones impuestas disponen de un plazo de prescripción que varía en función del tipo de sanción y su gravedad. Asimismo, el *dies a quo* se empieza a contar desde el día siguiente en que se puede ejecutar la resolución por la que imponga la sanción o bien,

cuando transcurra el plazo para recurrirla. Ahora bien, la prescripción podrá ser interrumpida por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo cuando se encuentre paralizado durante más de seis meses por causas no imputables al infractor. En ese sentido, las sanciones impuestas prescriben en los siguientes plazos: a) prescriben en el plazo de un año, las sanciones por importe igual o superior a 40.000 euros; b) prescriben en el plazo de 2 años, las sanciones por importe comprendido entre 40.001 y 300.000 euros; c) prescriben en el plazo de 3 años, las sanciones por importe superior a 300.000 euros.

3. Conclusiones

Tras haber analizado en profundidad las publicaciones y estudios de juristas y expertos en protección de datos y haber estudiado la jurisprudencia de los tribunales españoles y europeos juntamente con informes y resoluciones de la AEPD, he llegado a las siguientes conclusiones que se pueden extraer del contenido de este trabajo.

I) En primer lugar, del estudio realizado se desprende que los trabajadores son sujetos interesados en el tratamiento de datos de carácter personal cuya responsable del tratamiento es la empresa en la que prestan servicios. En ese sentido, tanto el RGPD como la LOPD han reconocido que los trabajadores deben estar protegidos de las intromisiones ilícitas y de la obtención y tratamiento injustificadas en los datos de carácter personal por parte de la empresa. De tal manera, las empresas pueden obtener datos de los trabajadores siempre y cuando esté justificado y se informe a los afectados de la finalidad del tratamiento.

II) En segundo lugar, reconociendo al trabajador como persona interesada o afectada en el tratamiento de datos personales, tanto el RGPD como la LOPD le otorgan una serie de derechos a fin de poder garantizar la no vulneración de sus derechos y, en particular, el derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen. Estos derechos que pueden ejercer cualquier trabajador se sintetiza en los derechos de información, acceso, portabilidad, rectificación, supresión, bloqueo y oposición. A su vez, se establece una serie de obligaciones a la empresa a fin de garantizar dichos derechos.

III) El factor del consentimiento en el tratamiento de datos se convierte en fundamental para la protección de datos de carácter personal de los trabajadores. En ese sentido, tanto la jurisprudencia como los criterios de los organismos de protección de datos y la doctrina de juristas y expertos consideran que el consentimiento del trabajador es un asunto controvertido. Sin embargo, la doctrina mayoritaria considera acertado que el consentimiento ha sido concedido mediante el contrato de trabajo. No obstante, en relación con la aplicación de

sistemas de video-vigilancia en centros de trabajo requieren de otros requisitos no siendo suficiente el consentimiento dado mediante el contrato de trabajo.

IV) La instalación de sistemas de video-vigilancia en los centros de trabajo ha provocado que el legislador tanto europeo como nacional adopte medidas a fin de garantizar los derechos de los trabajadores. En ese sentido, la propia LOPD contempla la posibilidad de instalación de sistemas de captación de imágenes. Si la norma general en el tratamiento de datos es que para que sea lícito debe haber consentimiento previo, en el caso de la obtención de datos de carácter personal mediante sistemas de video-vigilancia en centros de trabajo el factor de la proporcionalidad es de vital importancia según la doctrina mayoritaria. De tal manera, la proporcionalidad de la medida garantizará que los trabajadores no vean vulnerados sus derechos mientras realizan sus funciones laborales. No hay que olvidar que el propio ET reconoce que la empresa podrá adoptar las medidas que considere oportunas para el control y vigilancia conforme los trabajadores realizan correctamente sus tareas.

   De igual forma que la proporcionalidad es un factor determinante para considerar lícita la obtención de datos mediante sistemas de video-vigilancia, el derecho de información de los trabajadores también es esencial. En ese sentido, tanto la jurisprudencia como la doctrina coinciden en que el trabajador debe estar informado de la existencia de cámaras en el centro de trabajo considerando ilícita la captación de imágenes sin haber informado previamente o habiendo ocultado las cámaras a fin de que los trabajadores desconozcan de su funcionamiento.

V) Uno de los objetivos marcados era analizar hasta qué punto las imágenes captadas podían ser utilizadas. En ese sentido, según ha manifestado la jurisprudencia, las imágenes captadas por los sistemas de video-vigilancia podrán ser utilizadas para aquellas finalidades para las que se hubieran previsto. De esta manera, en caso de que la empresa hubiera instalado sistemas de video-vigilancia para el control de accesos, no serviría para sancionar a trabajadores en materia laboral ya que la finalidad no era esa. Sin embargo, la jurisprudencia ha considerado que en caso de que se cometieran delitos y las cámaras captaran las imágenes, estas podrían ser

utilizadas como prueba en el procedimiento judicial correspondiente. Es decir, dichas imágenes servirían para un procedimiento penal pero no para un procedimiento de la jurisdicción social. Por tanto, la adopción de medidas para el control y vigilancia del cumplimiento de las tareas de los trabajadores mediante la instalación de sistemas de video-vigilancia únicamente serán lícitas cuando se haya informado de dicha finalidad.

VI) Finalmente, en cuanto a la responsabilidad civil de los responsables del tratamiento, la ley prevé que cuando se produzca una infracción en el tratamiento de datos personales el responsable deberá indemnizar a los afectados por los daños y perjuicios provocados. Estos daños, considera la doctrina, deberán ser efectivos, reales, evaluables económicamente e individualizables. Ahora bien, tal y como se ha podido analizar, existe controversia en relación con el tipo de responsabilidad ya que por un lado se entiende que debe existir dolo en la comisión de la infracción que provoque los daños y perjuicios y, por otro lado, hay doctrina que considera que se trata de una responsabilidad objetiva, es decir, que existe responsabilidad independientemente de la culpa del responsable. A mayor abundamiento, la ley prevé un sistema sancionador de carácter administrativo en los casos de la comisión de infracciones en materia de protección de datos.

Referencias bibliográficas

Bibliografía básica

ÁLVAREZ HERNANDO, J. Las relaciones laborales y la protección de datos. Pamplona. Aranzadi, 2017.

BAZ RODRÍGUEZ, JESÚS. Privacidad y protección de datos de los trabajadores en el entorno digital. Madrid. Editorial Bosch, 2019.

BLÁZQUEZ AGUDO, E.

- Aplicación práctica de la protección de datos en las relaciones laborales. Madrid. Wolters Kluwers, 2018.
- Novedades laborales en la nueva Ley Orgánica de protección de datos. Trabajo y Derecho, nº 50, 2019.

DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.

- Control informático, video-vigilancia y protección de datos en el trabajo. Valladolid. Lex Nova, S.A.U., 2012.
- <<Protección de datos y contrato de trabajo>>. Justicia Laboral, nº 46, 2011.

FERRER SERRANO, ROBERTO L. Guía de protección de datos de los trabajadores. Valencia. Tirant lo Blanch, 2019.

GARCIA MURCIA, J.M. y RODRIGUEZ CARDO, I.A. La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo. Revista Española de Derecho del Trabajo, nº 216, 2019.

GIL MEMBRADO, C. Video-vigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado. Madrid. La Ley, 2019.

GONZÁLEZ GONZÁLEZ, CARLOS. Guía práctica sobre protección de datos: ámbito laboral. Navarra. Aranzadi, 2019.

GOÑISEIN, J.L. La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa. Albacete. Bomarzo, 2018.

HERNÁNDEZ 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. Madrid. Reus, 2016.

LEFEBVRE, FRANCIS. Memento Práctico Social 2021. Madrid. Francis Lefebvre, 2021.

LÓPEZ ÁLVAREZ, L.F. Protección de datos personales: adaptaciones necesarias al nuevo Reglamento Europeo. Madrid. Francis Lefebvre, 2016.

MERCADER UGUINA, J.R. Protección de datos y garantía de los derechos digitales en las relaciones laborales. 3ª ed. Madrid. Francis Lefebvre, 2019.

ORELLANA CANO, ANA Mª. El Derecho a la protección de datos personales como garantía de la privacidad de los trabajadores. Navarra. Aranzadi, 2019.

PIÑAR MAÑAS, J.L. Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos digitales. Pamplona. Aranzadi, 2019.

PRECIADO DOMÈNECH, CARLOS HUGO. Los derechos digitales de las personas trabajadores. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos Digitales. Pamplona. Aranzadi, 2019.

RECIO GAYO, M. Nuevo Dictamen del GT29 sobre tratamiento de datos en el trabajo: el interés legítimo. Diario La Ley, nº 8, Sección Ciberderecho, 19 de julio 2017.

RODRÍGUEZ ESCANCIANO, S. Video-vigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Diario La Ley, nº 9328, 2 de enero de 2019.

SERRANO OLIVARES, R. Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, IUSLabor 3/2018.

TASCÓN LÓPEZ, R. El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión. Madrid. Civitas, 2005.

TRONCOSO REIGADA, A. La protección de datos personales en el ámbito laboral, en VV.AA. La protección de datos personales en busca del equilibrio. Valencia. Tirant lo Blanch, 2010.

TRUJILLO MACHUCA, V. La reclamación de daños y perjuicios en materia de protección de datos. Actualidad Civil, nº 12, Sección Persona y derechos / A fondo, diciembre 2020, Wolters Kluwer. La Ley 15088/2020.

VALVERDE ASENCIO, A.J. Protección de datos de carácter personal y derechos de información de los representantes de los trabajadores. Temas laborales, nº 118, 2013.

Bibliografía complementaria

Agencia Española de Protección de Datos

- Resolución R/00035/2006, de 27 de febrero de 2006.
- Informe 0533/2006
- Informe 0494/2008
- Informe 0006/2009
- Informe 0173/2009
- Informe 0495/2009
- Informe 0227/2010
- Informe 0333/2012
- Informe 0475/2014

Grupo del art. 29

- Dictamen 8/2001, de 13 de septiembre de 2001.
- Dictamen 1/2010, de 16 de febrero de 2010.
- Dictamen 15/2011, de 13 de julio de 2011.
- Directrices sobre los delegados de protección de datos (DPD), de 13 de diciembre de 2016, revisadas y adoptadas por última vez el 5 de abril de 2017.
- Dictamen 2/2017, de 8 de junio de 2017.

Legislación citada

Carta de Derechos Fundamentales de la Unión Europea del Parlamento Europeo y la Comisión, de 7 de diciembre de 2000. DOCE 2000/C 364/01.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). DOUE L.119/1 (04-05-2016).

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DOCE núm. 281, de 23 de noviembre de 1995.

Proclamación interinstitucional sobre el pilar europeo de derechos sociales de 13 de diciembre de 2017. DOUE 2017/C 428/09.

Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea. DOUE 2012/C 326/01.

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. BOE núm. 115 (14-05-1982).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE. Núm 294 (06-12-2018).

Real Decreto Legislativo 2/2015, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. BOE núm. 255 (24-10-2015).

Jurisprudencia referenciada

TEDH, Sección Tercera, de 9-1-18 (Caso López Ribalda y Otros – Asuntos 1874/13 y 8567/13).

TJUE, Sala Tercera, de 24-11-11, ASNEF, C-468/10 y C-469/10.

TJUE, Sala Segunda, de 20-12-17, asunto Peter Nowak, C-434/16.

TC, Sala Primera, nº 254/1993, de 20 de julio de 1993, Rec. Amparo 1827/1990.

TC, Sala Segunda, nº 94/1998, de 4 de mayo de 1998, Rec. 840/1995.

TC, Pleno, 292/2000, de 30 de noviembre de 2000. Rec. Inconstitucionalidad 1463/2000.

TC, Sala Primera, nº 29/2013, de 11 de febrero de 2013, Rec. 10522/2009.

TC, Pleno, nº 39/2016, de 3 de marzo de 2016. Rec. Amparo 7222/2013.

TSJ Madrid, Sala de lo Contencioso-administrativo, Sección 9ª, nº 848/2000 de 16 de octubre de 2000, Rec. 1132/97.

SAN, Sala contencioso-administrativo, Sección 1ª, de 24 de enero de 2003, Rec. 400/2001.

SAN, Sala contencioso-administrativo, de 19 de marzo de 2014, Rec. 176/2012.

Listado de abreviaturas

AEPD	Agencia Española de Protección de Datos
AN	Audiencia Nacional
Art.	Artículo
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CEDH	Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales
Const.	Constitución
DPD	Delegado de Protección de Datos
ET	Estatuto de los Trabajadores
FJ	Fundamento Jurídico
GT29	Grupo del art. 29
LGSS	Texto Refundido de la Ley General de la Seguridad Social
LO	Ley Orgánica
LOLS	Ley Orgánica de Libertad Sindical
LOPD	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
LPRL	Ley de Prevención de Riesgos Laborales
RGPD	Reglamento del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TFM	Trabajo de Final de Máster

TJUE	Tribunal de Justicia de la Unión Europea
TSJ	Tribunal Superior de Justicia
UE	Unión Europea