Universidad de Valladolid

FACULTAD DE CIENCIAS SOCIALES, JURÍDICAS Y DE LA COMUNICACIÓN.

GRADO EN RELACIONES LABORALES Y RECURSOS HUMANOS

TRABAJO DE FIN DE GRADO

EQUILIBRIO ENTRE LA FACULTAD DE CONTROL EMPRESARIAL Y LA PROTECCIÓN DE DATOS DE LOS TRABAJADORES

Autora: Marta Tovar Álvarez

Dirigido por: María Carmen Gómez Torrego

Junio 2025

AGRADECIMIENTOS

Quiero dar las gracias a todas las personas que me han acompañado en este viaje, porque hoy cierro una etapa de mi vida, y lo hago rodeada de personas a las que quiero, admiro, y agradezco tener a mi lado.

En primer lugar, quiero agradecer todo el esfuerzo y apoyo que he recibido de mi tutora, Carmen. Gracias, porque sin tu ayuda nada de esto habría sido posible.

A mi familia, por depositar toda su confianza en mí y brindarme el amor de familia más puro. Por confiar en mí cuando ni yo misma lo hacía, y por acompañarme en cada paso que doy.

A mis amigas, porque han sido mi pilar en muchos momentos, por recordarme lo mucho que valgo día tras día y demostrarme que estarán a mi lado siempre, pase lo que pase.

A Elena, Manuela, Jimena y Laura porque nos hemos visto crecer, madurar, llorar y reír. Porque la vida os puso en mi camino cuando más os necesitaba, y habéis sido mi mayor descubrimiento.

A Gonzalo, por ser mi compañero de vida y mi mejor amigo. Por quererme como lo haces y demostrarme todos los días que estas orgulloso de la persona en la que me estoy convirtiendo.

A Segovia, por haber sido capaz de quedarte con un trocito de mi corazón. Gracias por poner en mi camino gente maravillosa y recuerdos que guardaré para siempre con todo el cariño del mundo.

A mí, porque este último año me he demostrado que todo sale adelante cuando hay esfuerzo de por medio.

Y por último a mi hermana, Cris. Mi mitad. Gracias por enseñarme lo que es luchar y no rendirse. Por enseñarme que los peores momentos también se deben afrontar con una sonrisa. Por ser mi cómplice y por querer siempre lo mejor para mí.

Os quiero.

RESUMEN

Este Trabajo de Fin de Grado aborda el conflicto entre dos intereses legítimos dentro de la relación laboral: por un lado, la facultad empresarial para organizar y controlar la actividad de los trabajadores; y por otro, el derecho de estos a proteger sus datos personales, reconocido como un derecho fundamental. A partir de esta tensión jurídica, el trabajo analiza cómo puede y debe ejercerse el poder de control empresarial sin vulnerar la intimidad y la dignidad de la persona trabajadora.

La investigación se centra especialmente en los efectos de las nuevas tecnologías y su uso generalizado en el ámbito laboral, lo que ha propiciado que los tratamientos de datos sean cada vez más frecuentes, complejos e intrusivos. En este contexto, el trabajo examina el marco normativo vigente en materia de protección de datos, tanto europeo como español.

A través de una revisión legal y doctrinal, complementada con resoluciones de la Agencia Española de Protección de Datos y jurisprudencia relevante, se estudian sistemas de control empresarial comunes como el uso de videovigilancia, sistemas biométricos, dispositivos de localización o controles de acceso. El objetivo principal es demostrar cómo el respeto al principio de proporcionalidad y la aplicación adecuada de las garantías legales permiten conciliar el control empresarial con la protección de los derechos fundamentales de los trabajadores.

PALABRAS CLAVE: *Protección de datos, control empresarial, trabajadores, privacidad y derechos.*

ABSTRACT

This Final Degree Project addresses the conflict between two legitimate interests within the employment relationship: on the one hand, the company's power to organise and control the activity of workers; and on the other, the right of workers to protect their personal data, recognised as a fundamental right. Based on this legal tension, the paper analyses how the company's power of control can and should be exercised without violating the privacy and dignity of the worker.

The research focuses particularly on the effects of new technologies and their widespread use in the workplace, which has led to increasingly frequent, complex and intrusive data processing. In this context, the work examines the current regulatory framework in the field of data protection, both European and Spanish.

Through a legal and doctrinal review, complemented with resolutions of the Spanish Data Protection Agency and relevant case law, it studies common business control systems such as the use of video surveillance, biometric systems, location devices or access controls. The main objective is to demonstrate how respect for the principle of proportionality and the appropriate application of legal safeguards make it possible to reconcile corporate control with the protection of workers' fundamental rights.

KEY WORDS: *Data protection, corporate control, workers, privacy and rights.*

ABREVIATURAS

AEPD Agencia Española de Protección de Datos

CE Constitución Española

CFT Corte Federal de Trabajo

DC Derecho Comparado

ET Estatuto de los Trabajadores

LOPD Ley Orgánica 5/1992 de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal

LOPDGDD Ley Orgánica, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales

LOPJ Ley Orgánica de Poder Judicial

LORTAD Ley Orgánica 5/1992 de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal

RAE Real Academia Española

RGPD Reglamento General de Protección de datos

SS Seguridad Social

STC Sentencia del Tribunal Constitucional

STS Sentencia del Tribunal Supremo

TEDH Tribunal Europeo de Derechos Humanos

TS Tribunal Supremo

ÍNDICE

1. INTRODUCCIÓN

1.1 Objetivo e hipótesis del trabajo

El objetivo principal de este trabajo es analizar como puede ejercerse el poder de control empresarial sobre la actividad laboral sin vulnerar los derechos fundamentales de protección de datos personales de los trabajadores. En concreto, se pretende estudiar hasta que punto es posible compatibilizar el poder de control del empleador con los límites del respeto a la intimidad y la dignidad de la persona.

Como hipótesis de partida, se plantea lo siguiente: si el poder de control empresarial se ejerce respetando los principios de proporcionalidad, minimización de datos y limitación de la finalidad, y conforme a la normativa vigente, es posible asegurar una armonización entre el interés legítimo de la empresa y los derechos fundamentales de los trabajadores.

Y de la misma forma, se presupone que la falta de información o el uso excesivo de herramientas de control puede derivar en prácticas que vulneren los derechos fundamentales, formando responsabilidades legales para las empresas.

1.2 Resumen sobre el estado de la cuestión

Hoy en día, el uso de las nuevas tecnologías en las empresas ha cambiado radicalmente la forma en la que se supervisa el trabajo. Herramientas como las cámaras de videovigilancia, los sistemas de geolocalización, controles biométricos…se han convertido en prácticas de supervisión empresarial habituales. Esta nueva situación ha provocado que muchas decisiones empresariales impliquen el tratamiento de datos personales de los trabajadores, por lo que se han generado ciertas tensiones entre la facultad de control empresarial y la protección de datos de estos.

Ante esta situación, la normativa vigente y el marco legal nacional se ha adaptado para responder a este escenario. A nivel europeo el Reglamento General de Protección de Datos, el cual ha supuesto un antes y un después al establecer ciertas normas altamente estrictas. Y a nivel nacional la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, donde se especifican aspectos generales relacionados con el ámbito laboral.

Por lo tanto, podemos decir que nos encontramos ante un panorama donde el avance tecnológico exige encontrar un equilibrio entre las empresas, las cuales están en su pleno derecho de organizar y proteger su actividad, y los trabajadores, quienes siguen teniendo derechos fundamentales que deben ser respetados.

1.3 Estructura empleada en el estudio

El trabajo se estructura de una forma coherente y clara. Comenzando por una introducción donde se exponen los objetivos y la hipótesis. A continuación, se desarrolla un marco teórico y normativo en el que se analizan los conceptos clave, los derechos de los trabajadores y mecanismos de control empresarial. Finalmente se presentan las conclusiones, donde se recogen las reflexiones finales, dando respuesta a las hipótesis planteadas.

2. MARCO TEÓRICO

2.1 Evolución histórica y marco normativo actual

La protección de datos personales en España ha experimentado una notable evolución a lo largo de las últimas décadas, principalmente por los grandes avances tecnológicos y el aumento de la preocupación de los ciudadanos por la intimidad respecto al uso de la información personal.

Desde las primeras referencias legales, hasta el actual marco jurídico ya consolidado, nuestro ordenamiento español ha experimentado varias etapas legislativas que han ido adaptándose, tanto a la realidad social de nuestro país como al contexto europeo:

- Ley Orgánica 5/1992 de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)

La LORTAD fue la primera norma española que reguló específicamente la protección de datos personales. Se dictó en cumplimiento de la Directiva 95/46/CE y marcó el inicio de una legislación propia en esta materia en España. Aspectos destacados:

- Limitaba su ámbito al tratamiento automatizado de datos, dejando fuera los ficheros manuales.
- Estableció los principios básicos de la protección de datos: calidad de los datos, legitimación del tratamiento, información al afectado, consentimiento y deber de secreto.
- Introdujo derechos para los ciudadanos: acceso, rectificación y cancelación de datos.
- Creó la Agencia de Protección de Datos como autoridad independiente de control.

- Ley Orgánica 15/1999, de protección de Datos de Carácter Personal (LOPD)

La LOPD derogó la LORTAD para ampliar el marco legal a todos los ficheros, automatizados o no, y adaptarse mejor a la directiva europea. Aspectos destacados:

- Ampliación del ámbito a ficheros no automatizados.
- Reforzamiento del principio del consentimiento como base general del tratamiento.
- Introducción de nuevas figuras: encargado del tratamiento.

- Regulación más detallada de los derechos ARCO: Acceso, Rectificación, Cancelación y Oposición.
- Fomento del uso de medidas técnicas y organizativas para garantizar la seguridad de los datos.

- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Este reglamento desarrolló la LOPD en materia de seguridad de los ficheros automatizados. Aspectos destacados:

- Clasificó los datos en tres niveles de seguridad (básico, medio y alto).
- Impuso medidas técnicas y organizativas proporcionales a la sensibilidad de los datos.
- Exigió la existencia de un documento de seguridad y controles de acceso.
- Supuso el primer intento serio de definir estándares mínimos de seguridad en los sistemas de tratamiento de datos.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Este Real Decreto completó y desarrolló la LOPD y reguló de forma más detallada aspectos relevantes tales como el consentimiento del titular de los datos, el deber de información por parte del responsable del tratamiento y la clasificación de las medidas de seguridad en función del nivel de sensibilidad de los datos. Esta nueva normativa fue de especial relevancia especialmente para las relaciones laborales, ya que se estableció la obligación empresarial de justificar el uso de determinados datos personales.

- Reglamento General de Protección de Datos (UE) 2016/697 (RGPD)

Este reglamento supuso un cambio estructural en la regulación de datos personales de la UE, y es de aplicación directa para todos los estados miembros desde el 25 de mayo de 2018. Este reglamento estableció unos principios esenciales:

- Trasparencia, minimización de datos y limitación de la finalidad.
- Sustitución de los derechos ARCO por los nuevos derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición.
- Regulación de figuras clave como el delegado de protección de datos.

- Eliminación de la obligación de registrar ficheros en la AEPD, sustituida por la evaluación de impacto y el registro interno de actividades de tratamiento.
- Aplicación extraterritorial: afecta a empresas fuera de la UE que traten datos de ciudadanos europeos.

- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

Esta ley adapta el derecho español al RGPD y desarrolla algunos aspectos nacionales. Aspectos destacados:

- Mantiene y adapta los derechos ARCO, alineándolos con los del RGPD.
- Reconoce derechos digitales como el derecho a la desconexión digital, la neutralidad de Internet, la educación digital o la protección de los menores en Internet.
- Regulación detallada del delegado de protección de datos y de su designación en ciertas entidades.
- Establece criterios claros para el tratamiento de datos en el ámbito laboral, educativo o sanitario.
- Introduce especificidades sobre el tratamiento de datos en videovigilancia, sistemas biométricos y uso de dispositivos digitales en el trabajo.

Con la LOPDGDD se completa la estructura de la normativa nacional actual, donde el RGPD constituye el marco general europeo y la LOPDGDD actúa como complemento de la normativa nacional, regulando aspectos en los que el Derecho de la Unión permite cierto margen de maniobra a los Estados Miembros.

2.2 Concepto de tratamiento de datos personales

Para abordar con propiedad el tratamiento de datos personales en el marco de la protección de datos, resulta imperativo partir de una adecuada delimitación conceptual de lo que se entiende por "datos personales". Conforme al Reglamento (UE-9 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (en adelante RGPD) se considera dato personal cualquier información concerniente a una persona física identificable. En particular, en el artículo 4.1 del RGPD define a una *"persona física identificable*" como aquella cuya identidad pueda determinarse, directa o indirectamente, mediante identificadores tales como el nombre, un número de identificación, datos de localización, identificadores electrónicos o elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

En virtud de esta definición, cualquier dato que posibilite la individualización de una persona, se configura como dato personal. Ejemplo de ellos son el nombre y apellidos, la fecha de nacimiento, el domicilio, la dirección de correo electrónico o los datos de geolocalización. No obstante, el RGPD establece una diferenciación categorial dentro de los datos personales, distinguiendo entre los datos de naturaleza ordinaria y aquellos que revisten un carácter especial o sensible.

En este sentido, el artículo 9.1 del RGPD delimita el ámbito de datos personales de categoría especial, comprendiéndose dentro de esta clasificación aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como los datos genéticos, biométricos dirigidos a la identificación univoca de una persona, y los relativos a la salud, la orientación sexual…

Dado su carácter especialmente sensible, el tratamiento de estos datos se encuentra sujeto a un régimen jurídico reforzado, prohibiéndose su tratamiento salvo que concurra alguna de las excepciones previstas en el artículo 9.2.a-j del RGPD, entre las cuales encontramos:

a. La obtención del consentimiento explícito del interesado, salvo que el Derecho de la Unión o de los Estados Miembros lo prohíba expresamente.
b. La necesidad de tratamiento para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral, la Seguridad Social (en adelante SS) y la protección social, en la medida en que lo autorice el Derecho de la Unión o de los Estados Miembros.
c. La protección de intereses vitales del interesado o de otra persona física cuando este se encuentre incapacitado para otorgar su consentimiento
d. El tratamiento efectuado en el marco de actividades legítimas de entidades sin ánimo de lucro con fines políticos, filosóficos, religiosos o sindicales, siempre que dicho tratamiento se realice en el ámbito de sus actividades legítimas y con garantías adecuadas.
e. La manifestación pública y voluntaria de dichos datos por parte del propio interesado
f. La necesidad de tratamiento para la formulación, el ejercicio o la defensa de reclamaciones, en el contexto de procedimientos judiciales o administrativos
g. La existencia de un interés público esencial que justifique el tratamiento, siempre que se salvaguarden los derechos y libertades fundamentales del interesado

h. La utilización de dichos datos para la evaluación de la capacidad laboral del trabajador, el diagnostico médico, la prestación de asistencia sanitaria os social, o la gestión de sistemas y servicios de salud
i. La necesidad del tratamiento por razones de interés público en el ámbito de la salud pública, incluyendo la prevención de amenazas sanitarias graves y la garantía de estándares elevados en la calidad y seguridad de la asistencia sanitaria
j. El tratamiento con fines de investigación científica, histórica o estadística, sujeto a la aplicación de medidas técnicas y organizativas adecuadas para la protección de los derechos del interesado

Desde una perspectiva laboral, el RGPD faculta a los Estados Miembros para desarrollar normativas específicas que garanticen la protección de los derechos y libertades de los trabajadores en el tratamiento de sus datos personales en el contexto de la relación laboral.

Dichas disposiciones pueden abarcar desde la fase precontractual, el desarrollo de la prestación laboral, hasta el fin de esta, incluyendo aspectos como la promoción de la igualdad y la diversidad, la protección de la seguridad y salud en el trabajo, la gestión del rendimiento y la monitorización del trabajador en el ejercicio de sus funciones (AEPD, 2021)

Por ejemplo, en España, en el artículo 87 de la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (en adelante LOPDGDD) establece reglas sobre el uso de sistemas de videovigilancia en el trabajo. Indica que los empleados deben ser informados de su instalación y que las imágenes solo pueden usarse para la seguridad o el control de la relación laboral, sin afectar la intimidad del trabajador.

No obstante, el RGPD introduce una excepción fundamental en su ámbito de aplicación, estableciendo en su artículo 2.2.c que no estarán sujetas a la normativa de protección de datos aquellas actividades *"exclusivamente personales o domésticas"* entendiendo como actividades "exclusivamente personales o domésticas" aquellas que se llevan a cabo en el contexto de la vida privada y familiar del individuo, sin conexión alguna con una actividad profesional o comercial.

2.3 Principios legales para el trato con datos personales

El artículo 5 del RGPD regula los principios legales relativos al tratamiento de los datos personales. Estos principios son los siguientes:

a. Licitud, lealtad y transparencia. Según el artículo 5.1.a del RGPD, los datos personales deben ser tratados de forma licita, real y transparente con el afectado para respetar la legalidad vigente y realizarse de manera honesta para ofrecer al titular de los datos una información clara y accesible sobre cómo se gestionan sus datos personales.
b. Limitación de la finalidad: este principio consagrado en el articulo 5.1.b del RGPD establece que los datos personales deben ser "*recogidos con fines determinados, explícitos y legítimos, y no podrán ser tratados ulteriormente de manera incompatible con dichos fines iniciales"*. Cabe destacar, no obstante, que el precepto en cuestión establece una excepción relevante: el tratamiento subsiguiente de datos personales para archivado de interés público, investigación científica o histórica, o para fines estadísticos, conforme a lo estipulado en el artículo 89.1 del mismo reglamento, no se estimará incompatible con los objetivos primarios para los que tales datos fueron obtenidos
c. Minimización de datos. Este principio establece que solo se podrán tratar los datos *"adecuados, pertinentes y limitados a lo necesario"*. Este derecho viene recogido en el Derecho Comparado (en adelante DC), dentro del artículo 32 de la Ley Federal alemana para la Protección de Datos de 30 de junio de 2017, en el cual denomina a este principio *"principio de última ratio"*, definido por la Corte Federal de Trabajo (en adelante CFT) (Ana Orellana, 2019)
d. Exactitud. Recogido en el artículo 5.1.d del RGPD, exige que los datos personales objeto de tratamiento sean veraces y exactos y, en caso necesario, estén actualizados. Para ello, y en caso contrario, el responsable de tratamiento deberá adoptar todas aquellas medidas que garanticen que los datos que resulten inexactos, atendiendo a los fines para los que fueron recabados, sean suprimidos o corregidos sin demora.
e. Limitación del plazo de conservación. De acuerdo con este principio previsto en el artículo 5.1.e del RGPD los datos personales deben almacenarse de manera que permita la identificación del interesado únicamente durante el tiempo estrictamente necesario para cumplir con las finalidades que motivaron su recogida y tratamiento, sin perjuicio de que sean admitida su

conservación por periodos más prolongados cuando el tratamiento posterior se realice exclusivamente con fines de archivo en interés público, investigación científica o histórica, con fines estadísticos, siempre que respeten las garantías establecidas en el artículo 89.1 del mismo reglamento. En estos casos deben aplicarse las medidas técnicas y organizativas adecuadas para salvaguardar los derechos y libertades fundamentales del interesado.

f. Integridad y confidencialidad. Recogido en el artículo 5.1.f del RGPD, establece la obligación de tratar los datos personales garantizando su protección frente a accesos no autorizados, usos ilícitos o cualquier forma de alteración, perdida, destrucción o daño accidental.
g. Responsabilidad proactiva. Finalmente, según lo dispuesto en el artículo 5.2 del RGPD, el responsable del tratamiento de datos personales será el responsable del correcto cumplimiento de lo establecido en el artículo 5.1, y deberá ser capaz de demostrarlo.

Es por ello por lo que, todos los principios enunciados configuran un marco normativo completo, en el cual no solo guían el tratamiento de datos personales, sino que establecen una exigencia de diligencia y demostrabilidad para el responsable del tratamiento, garantizando de esta forma la tutela efectiva de los derechos fundamentales de los interesados.

2.4 Sujetos esenciales en materia de protección de datos.

El RGPD ha formado un marco jurídico común en toda la Unión Europea, con el objetivo de garantizar un elevado nivel de protección de los datos personales. En toda la legislación y estructura normativa, cabe destacar tres sujetos esenciales dentro de la materia de protección de datos, cuyas funciones son imprescindibles para el control y responsabilidad en el trato de datos personales de las personas trabajadoras (García Hernández, 2022). A continuación, se ha referencia a cada uno de ellos, explicando posteriormente sus diferencias en una tabla de elaboración propia:

2.4.1 Responsable de tratamiento de datos personales.

El responsable de tratamiento, también denominado como "responsable", viene definido por el RGPD tal y como se indica a continuación: *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del*

tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

De la propia definición podemos destacar varios elementos esenciales. En primer lugar, la personalidad jurídica, pudiendo ser esta tanto persona física como jurídica. En segundo lugar, el ejercicio de la actividad pudiendo realizarse de una forma tanto individual como colectiva, sin perjuicio de que se trate de una entidad tanto pública como privada. Sin embargo, existe un elemento el cual contiene una mayor importancia jurídica: el cometido atribuido al responsable del tratamiento (García Hernández, 2022):

- Determinar la finalidad del tratamiento de datos personales, es decir, "para qué" se tratan dichos datos.
- Establecer la forma en que se procesarán los datos, es decir, "cómo" se llevara a cabo dicho tratamiento.

En la misma línea, el RGPD, en su artículo 24, regula las obligaciones del responsable del tratamiento, articuladas en tres apartados diferentes, de los cuales podemos extraer de su contenido las siguientes responsabilidades:

- El responsable del tratamiento deberá adoptar todas las medidas necesarias para asegurarse del correcto cumplimiento del presente reglamento, las cuales se actualizarán y revisarán cuando sea conveniente.
- Deberá adoptar cuando considere necesario las políticas de protección de datos que considere oportunas.
- El responsable del tratamiento podrá demostrar el cumplimiento de sus obligaciones mediante adhesión a códigos de conducta o mecanismos de certificación aprobados.

2.4.2 Encargado de tratamiento de datos personales.

De la misma manera, el encargado de tratamiento, también denominado "encargado", viene definido por el RGPD con la siguiente definición: *"la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".*

De la propia definición del encargado, podemos realizar una comparativa con la figura del responsable del tratamiento. Ambos sujetos comparten una posición funcional en el ámbito de la protección y el tratamiento de datos personales, si bien con una diferencia esencial en cuanto a sus competencias y el nivel de decisión.

El encargado actúa por cuenta del responsable, limitándose a ejecutar las operaciones de tratamiento conforme a las instrucciones precisas que dicho sujeto le imparta, sin gozar de autonomía para determinar los fines ni os medios del tratamiento.

Es por ello por lo que toda intervención realizada por el encargado de tratamiento está directamente subordinada a lo establecido por el responsable.

Las obligaciones del encargado de tratamiento se diferencian en tres bloques diferentes (García Hernández, 2022):

- Obligaciones organizativas: el encargado carece de facultad para decidir individualmente sobre la finalidad del tratamiento de datos, debiendo este limitarse a ejecutar las instrucciones impartidas por el responsable del tratamiento.
- Obligaciones de seguridad: le corresponde al encargado establecer mecanismos que aseguren la confidencialidad y la integridad de los datos tratados.
- Obligaciones de asistencia: deberá tratar con el responsable de forma directa, facilitando toda la asistencia necesaria para el correcto cumplimiento de las obligaciones en materia de protección de datos, quedándole prohibido transferir datos personales a terceros sin autorización, atendiendo a los derechos de acceso, rectificación, supresión y oposición de los interesados.

Además, atendiendo al artículo 28.3 del RGPD, le quedan atribuidas al encargado de tratamiento las siguientes funciones:

a. Tratará los datos personales bajo las instrucciones del responsable.
b. Garantizara que toda aquella persona autorizada para tratar los datos personales, estén comprometidas con el deber de confidencialidad.
c. Implementara medidas que aseguren la seguridad en el trato de datos personales.
d. Asistirá al responsable con las medidas necesarias para lograr el cumplimiento de los objetivos en materia de protección de datos.
e. Cooperara con el responsable para la consecución de sus deberes.
f. Eliminará o devolverá los datos personales al final de los servicios prestados, y conservará los datos en caso de solicitud de conservación por parte del Derecho de la Unión o de los Estados Miembros.

Con el fin de demostrar la correcta ejecución de sus obligaciones, el responsable tendrá acceso a toda la información pertinente que el encargado le proporcione, quien también deberá realizar las auditorías y comprobaciones necesarias.

2.4.3 Delegado de protección de datos

El delegado de protección de datos, uno de los sujetos de mayor importancia en materia de protección de datos, está regulado en los artículos del 34 al 37 de la LOPDGDD. Para comenzar, seguiremos el orden de la propia ley, comenzando por la designación del delegado de protección de datos. La normativa nacional relativa a la protección de datos impone en su artículo 34 la obligación de designar un delegado de protección de datos a los responsables y a los encargados del tratamiento, según lo dispuesto en el artículo 37.1 del RGPD. Sin embargo, además de lo establecido en dicho artículo, la legislación vigente amplia esta exigencia a una serie de entidades donde se incluyen:

- Los colegios profesionales.
- Instituciones educativas de cualquier nivel (públicas o privadas).
- Operadores de telecomunicaciones.
- Entidades del sistema financiero (bancos, aseguradoras…)
- Comercializadoras de energía o gas.
- Centros sanitarios con obligación de mantenimiento de historiales clínicos.
- Empresas del sector de la seguridad privada.
- Federaciones deportivas responsables de datos de menores.

Además de los casos en los que la designación de un delegado de protección de datos sea imperativa, cualquier entidad que trate con datos personales puede designar voluntariamente un delegado, quedando este, sujeto a la normativa vigente. En cualquiera de los dos casos de asignación voluntaria u obligatoria, dicha designación (así como cualquier modificación o cese) deberá notificarse a la AEPD o a la autoridad autonómica competente, en un plazo máximo de 10 días.

Las autoridades de control son las responsables de mantener y publicar un registro actualizado y accesible electrónicamente de los delegados de protección de datos designados. Además, los responsables y encargados podrán decidir sobre la dedicación parcial o total del delegado, en función de la complejidad y el volumen de las operaciones, y atendiendo a la naturaleza sensible de los datos tratados, o incluso el riesgo que puedan entrañar para los derechos y libertades de los interesados.

Continuando por el artículo 35, referente a la cualificación del delegado de protección de datos, el delegado, ya sea una persona física o jurídica, debe contar con conocimientos jurídicos y técnicos suficientes, tal y como se exige en el artículo 37.5 del RGPD.

Dicha cualificación podrá ser acreditada mediante mecanismos voluntarios de certificación, valorándose en este aspecto especialmente la posesión de titulación universitaria que garantice conocimientos específicos en materia de protección de datos

En cuanto a la posición del delegado de protección de datos recogido en el artículo 36 de la LOPDGDD, hace referencia a este como la conexión y vínculo entre la AEPD o las autoridades correspondientes y el responsable o encargados de tratamiento, estando este facultado para revisar procedimientos relacionados con el tratamiento de datos personales, así como proponer medidas para un adecuado cumplimiento de la normativa vigente.

Cuando el delegado de protección de datos forme parte de la estructura interna de la organización, este deberá garantizarse su independencia funcional. Es por ello por lo que no podrá ser objeto de sanción ni cese como consecuencia del ejercicio legítimo de sus funciones, salvo en casos de negligencia grave o dolo.

Además, para el desempeño de sus funciones, se deberá facilitar al delegado de protección de datos toda aquella información y procesos, sin que puedan oponérsele deberes de confidencialidad internos.

En el caso de que el delegado detecte cualquier infracción relevante en materia de protección de datos, tendrá este la obligación de poner los hechos en conocimiento de inmediato frente a los órganos correspondientes y al responsable o encargado de tratamiento, debiendo quedar constancia documentada de dicha actuación.

Para finalizar, es importante conocer la intervención del delegado de protección de datos en caso de reclamaciones ante autoridades de protección de datos recogido en el artículo 37 de la LOPDGDD.

Este precepto establece que, cuando exista un delegado de protección de datos designado por el responsable o encargado de tratamiento, la persona afectada podrá optar por acudir inicialmente a dicha figura de la entidad contra la que este quisiera reclamar antes de interponer una reclamación ante la AEPD o la autoridad correspondiente.

En tal caso, el delegado de protección de datos deberá trasladar su resolución al interesado en un plazo máximo de dos meses desde la recepción de la queja.

En el supuesto en el que la persona afectada acuda desde un inicio a la AEPD o a la autoridad correspondiente, estas podrán derivar la reclamación a su delegado de protección de datos, el cual dispondrá de un mes para emitir y comunicar una respuesta.

Si no lo hace transcurrido dicho plazo, la administración continuará con el procedimiento conforme a lo establecido en la normativa aplicable, concretamente según lo dispuesto en el Título VIII de esta LOPDGDD

A continuación, se expone una tabla de elaboración propia con las diferencias principales entre estos sujetos:

Aspecto	***Responsable del tratamiento***	***Encargado del tratamiento***	***Delegado de protección de datos***
Definición	*Persona o entidad responsable de la toma de decisiones sobre el tratamiento de los datos personales.*	*Persona o entidad que trata los datos personales siguiendo las instrucciones del responsable del tratamiento.*	*Persona física o jurídica que supervisa y asesora sobre el correcto cumplimiento de la normativa de protección de datos, y enlace con la AEPD*
Función principal	*Determinar el "para qué" y el "cómo" se tratarán los datos personales.*	*Ejecuta el tratamiento según lo indicado por el responsable del tratamiento.*	*Vigilar el correcto cumplimiento de la normativa y comunicarse con la AEPD.*
Capacidad de decisión	*Capacidad de decisión total sobre el tratamiento.*	*Sin capacidad de decisión, solo ejecuta las decisiones del responsable*	*No tiene capacidad de decisión, pero si puede recomendar y avisar sobre incumplimientos.*
Obligaciones	*Garantizar el correcto tratamiento del RGPD y aplicar medidas de seguridad.*	*Seguir las instrucciones del responsable y mantener la seguridad y confidencialidad*	*Supervisar y asesorar sobre el cumplimiento y ser el canal de contacto con las autoridades correspondientes*
Nombramiento	*No es "nombrado" formalmente: es la propia entidad (persona física o jurídica, pública o privada) quien decide su nombramiento.*	*Lo nombra el responsable.*	*Es designado por el responsable o el encargado del tratamiento, de forma obligatoria en los casos previstos en el artículo 37.1 del RGPD y artículo 34 de la LOPDGDD, o de forma voluntaria. La designación debe notificarse a la AEPD en un plazo máximo de 10 días.*
Base legal	*Artículo 24 del RGPD y Título V Capítulo I de la LOPDGDD*	*Artículo 28 del RGPD y Título V Capítulos I y II de la LOPDGDD*	*Artículos del 37 al 39 del RGPD y 34 al 37 de la LOPDGDD*
Responsabilidad legal	*Sí responde ante posibles infracciones.*	*Responde solo si incumple con las instrucciones o actúa de forma indebida.*	*No responde directamente, salvo negligencia grave o dolo.*
Relación con la AEPD	*Puede ser requerido por la AEPD para demostrar el correcto cumplimiento del RGPD.*	*No tiene relación directa con la AEPD, pero también puede ser evaluado si hay incumplimientos.*	*Es el principal contacto entre las organizaciones y la AEPD.*

Nota: tabla de elaboración propia.

2.5 El derecho de información del tratamiento de datos personales al interesado.

El derecho de información sobre el tratamiento de datos personales de los trabajadores, en cuanto al alcance, contenido mínimo y modalidades de entrega, se ha convertido en uno de los aspectos más conflictivos y litigiosos en el ámbito laboral y de protección de datos, generando un intenso debate doctrinal aun carente de una jurisprudencia completamente homogénea.

Bajo el actual marco establecido por el RGPD, esta exigencia informativa se erige en un derecho subjetivo del interesado, de manera que el responsable del tratamiento queda compelido a garantizar al trabajador un conocimiento cabal, claro y accesible de todas las operaciones efectuadas con sus datos (Ana María Orellana, 2019).

Dicha obligación atiende al principio de transparencia y forma parte inseparable del principio de responsabilidad proactiva, al imponer al responsable la carga de demostrar ante la autoridad de control y ante el propio interesado la correcta y continua prestación de la información correspondiente (Ana María Orellana, 2019).

Mientras que la LOPDGDD solo se refiere al contenido, el RGPD regula la forma y el contenido del derecho del interesado a la información del tratamiento de sus datos personales.

2.5.1 Forma de la información

En cuanto a la forma de la información de datos personales, la cual debe facilitar el responsable del tratamiento, viene recogido en el artículo 12 del RGPD en sus apartados primero y séptimo, en los cuales viene establecida la forma en la que ha de revestir la información. En ellos viene especificado lo siguiente:

- El responsable de tratamiento deberá tomar las medidas necesarias para facilitar al interesado toda la información recogida en los artículos 13 y 14 de este reglamento, *"de forma concisa, transparente, inteligible y de fácil acceso y con un lenguaje claro y sencillo",* especialmente si va dirigida a un niño.
- La entrega de la información al interesado podrá efectuarse utilizando medios tradicionales como el formato escrito o a través de herramientas electrónicas. En los casos en que la persona afectada lo solicite expresamente, será posible transmitir dicha información de forma verbal, siempre y cuando, con carácter previo, se haya verificado

su identidad por medio de algún procedimiento alternativo que ofrezca garantías suficientes.

- Por último, en virtud de lo previsto en los artículos 13 y 14, la información dirigida al interesado podrá conformarse mediante una combinación de texto e iconografía normalizada, teniendo como objetivo facilitar una percepción inmediata, clara y accesible del tratamiento proyectado. Esta iconografía deberá diseñarse conforme a los estándares oficiales, de forma que resulte fácilmente reconocible y comprensible. En el caso de su uso en soportes técnicos deberá ser susceptible de lectura mecánica por sistemas automatizados, garantizando así su plena eficacia.

2.5.2 Contenido de la información

Tanto el RGPD y la LOPDGDD distinguen el contenido de la información cuando se obtengan datos personales a través del interesado. Es por ello por lo que, en el momento de la obtención de estos datos, el responsable del tratamiento deberá facilitarle a este toda la información indicada a continuación, establecida en el artículo 13 del RGPD:

- Se deberá proporcionar al titular de los datos la identificación del responsable del tratamiento, incluyendo su nombre y formas de contacto, así como, si corresponde, los datos del representante legal.
- En caso de existir la figura del delegado de protección de datos, será necesario indicar quién es y cómo puede ser localizado.
- El propósito con el que se recogen los datos personales, así como señalar con qué fundamento jurídico se legitima su tratamiento.
- Si el tratamiento se basa en la existencia de un interés legítimo conforme al artículo 6.1.f) del RGPD, se deben detallar dichos intereses, ya sean propios del responsable o de terceros.
- Se deberá informar, si corresponde, sobre las personas o entidades a quienes se prevé comunicar los datos, ya sea identificándolas directamente o clasificándolas por categorías.
- Si los datos personales van a ser transferidos fuera del Espacio Económico Europeo, ya sea a terceros países o a organizaciones internacionales, deberá hacerse constar esta intención.
- Es preciso informar sobre el tiempo previsto para conservar los datos, y, si no es posible establecer una duración concreta, se explicarán los criterios empleados para determinar ese periodo.

- El interesado debe conocer los derechos que puede ejercer en relación con sus datos, como el acceso, la corrección de errores, la eliminación, la limitación del uso, la portabilidad y la oposición al tratamiento.
- Cuando el tratamiento tenga su base en el consentimiento expreso del interesado (art. 6.1.a o art. 9.2.a del RGPD), se le deberá comunicar que puede retirar dicho consentimiento en cualquier momento, sin consecuencias para la licitud previa del tratamiento.
- Se informará sobre la posibilidad de presentar una queja o reclamación ante la autoridad nacional de control en materia de protección de datos.
- En los casos en que la entrega de datos personales sea un requisito legal o contractual, deberá indicarse esta obligación y las posibles implicaciones negativas de no proporcionarlos.
- Por último, si los datos no han sido obtenidos directamente del propio interesado, el responsable deberá facilitar igualmente toda la información relevante prevista, cumpliendo el deber de información indirecta conforme al artículo 14 del RGPD, incluyendo los puntos recogidos en el artículo 13.

No obstante, el artículo 11 de la LOPDGDD limita su alcance a la mera exigencia de facilitar un medio de acceso (por ejemplo, una dirección electrónica) a la información restante, lo que resulta insuficiente y poco adecuada para garantizar plenamente la trasparencia del ejercicio de los derechos de los interesados (Ana María Orellana, 2019).

En estos casos específicos, la información básica deberá complementarse, además de con los extremos previstos en el artículo 13 del RGPD, con los siguientes elementos exigidos en el artículo 14 de este mismo reglamento:

- Las categorías de datos objeto de tratamiento
- Las fuentes de las que procedan los datos, y en su caso si proceden de fuentes de acceso público

2.6 Derechos de las personas trabajadoras respecto a sus datos personales

La protección de datos en el ámbito laboral constituye una cuestión de creciente relevancia, particularmente en el contexto de la digitalización y la intensificación del tratamiento de datos a través de sistemas de información sofisticados.

En este sentido, la entrada en vigor del RGPD ha instaurado un marco jurídico de obligado cumplimiento, orientado a la salvaguarda de los derechos fundamentales relacionados con la intimidad y la protección de datos de los trabajadores.

Con estas normativas lo que se pretende es evidenciar la necesidad de conciliar, de manera armónica, los intereses legítimos del empleador con los derechos inalienables de las personas trabajadoras para evitar de esta forma, en la medida de lo posible que se lleven a cabo prácticas que puedan resultar abusivas o contrarias a la buena fe contractual.

De esta forma y en virtud del RGPD las personas trabajadoras podrán ejercer los siguientes derechos de acuerdo con la propia ley, reconocidos en sus secciones segunda, tercera y cuarta.

No obstante, con carácter general, existe la posibilidad de que el responsable del tratamiento deniegue las solicitudes de las personas interesadas con el fin de ejercer estos derechos, conforme al artículo 12.5 del RGPD cuando sean consideradas infundadas o excesivas, especialmente por un carácter repetitivo. En mencionados casos, el responsable de tratamiento podrá según los apartados a) y b) del artículo 12.5 del RGPD (Ana maría Orellana, 2019):

- Cobrar un canon razonable, en función de los costes administrativos
- Negarse a actuar respecto a la solicitud

Los derechos de las personas trabajadoras son los siguientes:

2.6.1 Derecho de acceso

El derecho de acceso de los trabajadores viene recogido en el artículo 13 de la LOPDGDD y en el artículo 15 del RGPD. Es el derecho que tienen los interesados de poder acceder y obtener la información sobre el trato de sus datos personales y a conocer si se están tratando o no, y en tal caso derecho de acceso a esos datos personales y la siguiente información establecida específicamente en los apartados a)-h) del artículo 15 del RGPD:

a. Los propósitos concretos por los que se están utilizando los datos de carácter personal.
b. El tipo o clase de información personal que está siendo recopilada o manejada.
c. Las personas físicas, jurídicas o entidades a las que se hayan revelado o se prevea facilitar dichos datos, incluidas tanto terceras partes como organismos internacionales.

d. El periodo durante el cual se conservarán los datos, si se puede determinar, o bien los criterios aplicados para establecer dicha duración
e. El derecho que asiste a la persona afectada para solicitar al responsable del tratamiento la modificación, eliminación, restricción del uso, o incluso oponerse al mismo.
f. La posibilidad de acudir a la autoridad competente en materia de protección de datos para interponer una reclamación.
g. En los casos en los que la información personal no haya sido proporcionada directamente por el titular, información sobre su procedencia, en la medida que sea posible.
h. La existencia de decisiones que se hayan adoptado de manera automatizada sin intervención humana significativa.

En su apartado 2, el mismo precepto dispone que en caso de que se efectúen transferencias de datos personales a un tercer país u organización internacional, el interesado gozara del derecho a ser informado respecto de las garantías apropiadas que amparan dicha transferencia.

El apartado 3 reconoce al responsable la facultad de poner a disposición del titular una copia de los datos que sean objeto del tratamiento. Y por otra parte el artículo 13.2 de la LOPDGDD establece una presunción de cumplimiento de la petición de acceso cuando la responsable habilita para el interesado un mecanismo de acceso remoto que le permita consultar de modo continuo e integro sus datos; bastara a estos efectos, que el responsable comunique la modalidad de dicho acceso para que se considere satisfecha la solicitud de ejercicio del derecho de acceso.

La sentencia del Tribunal Europeo de Derechos Humanos (en adelante TEDH) de 13 de noviembre de 2012 (43932/2008), caso Joanna Szulc, considero vulnerado el derecho a la intimidad privada y familiar (artículo 8 del Convenio Europeo de Derechos Humanos) al no facilitarle al interesado el acceso al tratamiento de sus datos personales, por más de 10 años.

Asimismo, y sin perjuicio de lo establecido en la ley, se ha considerado relativo y no absoluto el derecho de acceso de los trabajadores, al plantearse la cuestión de si también las organizaciones sindicales ostentan el derecho de acceso a los datos personales de los trabajadores, dentro de su derecho a la información en la STS 111/2018 7 de febrero de 2018 (rcud 78/2017). En dicha sentencia el Tribunal Supremo (en adelante TS) confirmo el derecho que se les otorga a los sindicatos de acceder a información derivada del contrato de

trabajo, para el ejercicio de las funciones como cobertura de vacantes de los representantes de los trabajadores, concluyendo que el derecho a la protección de datos de los trabajadores no es absoluto (Ana maría Orellana, 2019).

2.6.2 Derecho de rectificación

Conforme a lo establecido en el artículo 16 del RGPD, el interesado tendrá derecho a rectificar los datos personales inexactos o completar un dato incompleto. Además, el artículo 14 de la LOPDGDD amplia este precepto estableciendo que el interesado deberá indicar concretamente en la solicitud el dato que desea sea rectificado y la corrección correspondiente, además de aportar la documentación que justifique la inexactitud o el carácter incompleto de los datos tratados, cuando sea necesario.

2.6.3 Derecho de supresión ("el derecho al olvido")

El RGPD reconoce en su artículo 17 a toda persona interesada el derecho a solicitar la eliminación de sus datos personales por parte del responsable que lo esté tratando, siempre que concurra alguna de las causas legalmente previstas. Dicha solicitud deberá atenderse sin demoras injustificadas cuando se den ciertas circunstancias concretas.

Entre las situaciones que justifican la supresión de los datos personales, se encuentran las siguientes:

a. Cuando los datos ya no sean pertinentes para los fines con los que fueron recabados o tratados con posterioridad
b. Que la persona afectada retire el consentimiento previamente otorgado, siempre que el tratamiento se haya fundamentado en dicho consentimiento y no exista otra base jurídica que lo sustente.
c. Cuando el titular de los datos se oponga a su tratamiento conforme a lo dispuesto en el artículo 21.1 del RGPD y no prevalezcan los intereses legítimos que justifiquen su mantenimiento.
d. En aquellos supuestos en los que los datos hayan sido tratados de forma contraria a la legalidad vigente.
e. Si la eliminación de los datos es necesaria para cumplir con una obligación legal derivada del derecho de la unión o de los ordenamientos jurídicos de los estados miembros

f. Cuando los datos personales se hayan obtenido en el marco de la prestación de servicios de la sociedad de la información dirigidos a menores, de acuerdo con lo establecido en el artículo 8.1

Asimismo, si los datos anteriormente mencionados han sido publicados previamente a nivel público, el responsable estará obligado a adoptar las medias razonables, siempre teniendo en cuenta el estado de la tecnología y los costes de su aplicación, para informar a otros responsables que estén tratando esa información sobre la solicitud de la supresión formulada por el interesado. Estas medidas incluirán acciones técnicas encaminadas a eliminar cualquier copia, enlace o reproducción de dichos datos.

No obstante, este derecho de supresión no será de aplicación cuando el tratamiento resulte necesario para alguno de los siguientes fines:

a. Para garantizar el ejercicio legítimo de los derechos fundamentales a la libertad de expresión y de acceso a la información.
b. Con el fin de cumplir con una obligación jurídica que recaiga sobre el responsable de tratamiento en virtud del Derecho de la Unión o de los Estados miembros, o cuando dicho tratamiento sea necesario para el cumplimiento de una función realizada en interés general o en el marco del ejercicio de potestades publicas conferidas a dicho responsable.
c. Por razones de relevancia en el ámbito de la salud pública, conforme a lo previsto en el artículo 9.2 letras h) e i), y en el apartado 3 del mismo precepto
d. Cuando el tratamiento persiga fines de archivo de interés público o tenga como objeto la investigación científica o histórica, así como la elaboración de análisis estadísticos
e. Para la interposición, desarrollo o defensa frente a reclamaciones de carácter jurídico.

2.6.4 Derecho a la limitación del tratamiento

Regulado en el artículo 18 del RGPD, se establece que el titular de los datos personales podrá ejercer su derecho a solicitar la restricción del tratamiento por parte del responsable cuando concurra alguna de las siguientes circunstancias:

a. Cuando el interesado impugne la veracidad o exactitud de los datos tratados, durante el tiempo necesario para que el responsable de tratamiento lleve a cabo las comprobaciones oportunas con el fin de verificar su exactitud
b. En aquellos casos en los que el tratamiento resulte contrario al derecho y el interesado en lugar de instar la supresión de los datos, opte por solicitar la restricción de su uso
c. Cuando los datos personales hayan dejado de ser necesarios para los fines que justificaron su recogida o tratamiento por parte del responsable, pero el interesado requiera su conservación con el propósito de ejercer, formular, o defenderse ante eventuales reclamaciones
d. Cuando el interesado haya ejercido su derecho de oposición con arreglo a lo previsto en el artículo 22.1 del RGPD y se halle pendiente la evaluación sobre la posible prevalencia de los intereses legítimos del responsable frente a los derechos y libertades de los interesados

Además, el responsable del tratamiento estará obligado a informar al interesado, de forma previa, acerca del levantamiento de la restricción acordada inicialmente en virtud del ejercicio de este derecho.

2.6.5 Derecho a la portabilidad de los datos

El titular de los datos tendrá derecho a obtener del responsable del tratamiento aquellos datos personales que le conciernan y que haya facilitado previamente, en un formato estructurado, de uso habitual e interpretación automatizada. Además, podrá solicitar su transmisión a otro responsable del tratamiento, sin que el responsable inicial pueda oponerse a dicha trasferencia siempre que concurran las siguientes causas:

- Que el tratamiento se base en el consentimiento explícito del interesado o que derive de una relación contractual.
- Que dicho tratamiento se lleve a cabo mediante procedimientos automatizados

Además, en el ejercicio de este derecho el interesado tiene la posibilidad de solicitar cuando sea técnicamente viable, que la portabilidad de los datos se realice directamente entre los responsables del tratamiento, sin necesidad de que los datos sean devueltos previamente al interesado.

Este derecho no será de aplicación cuando sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable de tratamiento, y no afectará negativamente a los derechos y libertades de otros según lo dispuesto en el artículo 20 del RGPD.

2.6.6 Derecho de oposición

En el artículo 21 del RGPD viene recogido lo siguiente:

1. El titular de los derechos personales tendrá la facultad de oponerse en cualquier momento por razones derivadas de su situación particular al tratamiento de sus datos cuando este se base en lo dispuesto en el articulo 6.1 letras e) o f), incluida la elaboración de perfiles fundamentada en esas mismas bases. Ante el ejercicio de este derecho, el responsable del tratamiento deberá cesar la utilización de estos datos, salvo que se pueda justificar la existencia de razones legitimas de especial relevancia que prevalezcan sobre los intereses, derechos y libertades del interesado, o cuando dicho tratamiento resulte indispensable para la interposición, ejercicio o defensa de reclamaciones ilegales.
2. Cuando el tratamiento de datos personales tenga como finalidad la mercadotecnia directa (definida esta por la RAE como "*conjunto de estudios y técnicas encaminados a favorecer la comercialización de productos y servicios*") el interesado tendrá derecho a oponerse en cualquier momento a que sus datos sean utilizados con tal finalidad, incluyendo la elaboración de perfiles, en la medida en que esté relacionado con la mencionada mercadotecnia.
3. En el caso de que el interesado ejerza su derecho de oposición frente al tratamiento de sus datos con fines de mercadotecnia directa, este deberá cesar de forma inmediata.
4. Este derecho deberá ser puesto en conocimiento del interesado de forma expresa, clara y diferenciada, y como máximo en la primera comunicación que se le remita.
5. Sin prejuicio de lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse a través de medios automatizados donde se apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica, histórica, o con fines estadísticos (artículo 89.1 del RGPD) el interesado para ejercer su derecho de oposición por motivos relacionados con su situación específica, salvo que dicho tratamiento sea indispensable para la ejecución de una misión fundamentada en razones de interés público.

2.6.7 Derecho a no ser objeto de decisiones individuales automatizadas

Según lo dispuesto en el artículo 22 del RGPD:

1. Cualquier persona titular de datos personales ostenta el derecho a no quedar sujeta a una decisión que se base exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles, cuando dicha decisión produzca efectos jurídicos sobre ella o le afecte de manera significativa de forma análoga.
2. La limitación descrita en el apartado anterior no será de aplicación cuando la decisión automatizada:
    a. Resulte necesaria para la formalización o ejecución de un contrato suscrito entre la persona interesada y el responsable del tratamiento.
    b. Se encuentre expresamente autorizada por la norma del DU o de los EEMM aplicable al responsable, siempre que dicha norma contemple también garantías apropiadas para la protección de los derechos, libertades e intereses legítimos del interesado.
    c. Se fundamente en el consentimiento expreso otorgado por el interesado.
3. En los supuestos contemplados en el apartado 2 letras a) y c), el responsable del tratamiento estará obligado a implantar salvaguardias adecuadas que protejan los derechos, libertades e intereses legítimos de la persona afectada. Entre dichas garantías deberán asegurarse, como mínimo, el derecho del interesado a obtener la intervención de una persona física por parte del responsable a manifestar su postura y a impugnar la decisión adoptada.
4. Las decisiones adoptadas en el apartado 2 no podrán sustentarse en categorías especiales de datos personales recogidas en el artículo 9.1, salvo que concurran las excepciones previstas en el apartado 9.2, y siempre que se hayan implementado medidas adecuadas que garanticen la salvaguarda de los derechos, libertades e intereses legítimos del interesado.

2.7 Control de la actividad laboral

2.7.1 Control de acceso a las instalaciones y centros de trabajo

El empleador está facultado para implementar mecanismos y sistemas de control de acceso a los centros e instalaciones de trabajo, sin que sea necesario obtener el consentimiento expreso de las personas trabajadoras, siempre que se protejan sus derechos fundamentales. (AEPD, 2021).

La base jurídica del tratamiento de datos se puede encontrar tanto en la ejecución del contrato de trabajo, basado en el artículo 20.3 del ET, donde se le reconoce al empleador la facultad empresarial de vigilancia y control, como en la satisfacción de un interés legítimo del empleador, en supuestos en los que la finalidad sea la protección de activos empresariales.

A modo ilustrativo la AEPD establece a modo de ejemplo una empresa donde se dispone de una sala donde se encuentran servidores con información sensible. En estos supuestos la implantación de un sistema de control que registre el acceso a dicho espacio resulta una medida idónea para cumplir con las obligaciones de seguridad impuestas por la normativa de protección de datos. En el momento de establecer este registro, será posible identificar qué personas accedieron a la sala en supuestos de accesos no autorizados, pérdidas o sustracciones de información, siempre que las personas trabajadoras hayan sido debidamente informadas de la existencia de dicho sistema y el tratamiento no resulte desproporcionado.

Es importante destacar que la monitorización constante y detallada de las entradas y salidas (si posteriormente se utiliza para fines diferentes a los iniciales como puede ser la evaluación del rendimiento laboral) excedería los límites permitidos y vulneraría el principio de limitación de la finalidad establecido en el artículo 5.1.b del RGPD.

Además, en cumplimiento del principio de minimización, se impone a los empleadores la obligación de estudiar y valorar la proporcionalidad y necesidad de los sistemas de control implantados, tratando de optar siempre por los sistemas menos intrusivos, cuando existan alternativas igualmente eficaces.

2.7.2 Videovigilancia

Según la Real Academia Española (en adelante RAE) el concepto de videovigilancia se define como: *"vigilancia por medio de un sistema de cámaras, fijas o móviles"*

La videovigilancia en el ámbito laboral constituye una manifestación del poder de dirección y control del empresario, reconocido en el artículo 20.3 del Estatuto de los Trabajadores. No obstante, su implementación y utilización deben adecuarse a los límites impuestos por el derecho fundamental a la protección de datos personales y a la intimidad de los trabajadores, garantizados por el artículo 18.1 de la CE, el RGPD y la LOPDGDD.

La videovigilancia en el ámbito laboral se ha consolidado como un instrumento indispensable para la prevención de riesgos, la protección del patrimonio de las empresas y la garantía de la seguridad en los centros de trabajo.

No obstante, tanto la adopción como la aplicación de esos sistemas de control se encuentran sujetos a un riguroso marco jurídico, marcando su propósito en equilibrar la necesidad de control y vigilancia con la protección de derechos fundamentales y la intimidad de los trabajadores. (AEPD, 2021)

En este sentido, la normativa vigente, en particular el RGPD y la LOPDGDD, impone el cumplimiento de principios esenciales tales como la proporcionalidad, la base jurídica, la finalidad legítima y la transparencia en el tratamiento de las imágenes captadas.

Las representaciones visuales que evidencien la identidad de un individuo son reconocidas jurídicamente como datos personales, puesto que, de acuerdo con la interpretación doctrinal y la normativa vigente, toda información que permite la identificación ya sea de forma directa o indirecta, se integra en el ámbito de protección de datos. (AEPD, 2021)

Este tratamiento de datos se regula en los artículos 22 y 89 de la LOPDGDD. Dichos artículos confieren a los empresarios la facultad de implementar dichos sistemas para ejercer funciones de control y supervisión, siempre dentro de los límites legales y bajo el principio de transparencia, exigiéndose la notificación previa y explicita a los trabajadores (o a los representantes en su caso).

Dicho tratamiento, en virtud de la ley, deberá llevarse a cabo con los siguientes requisitos:

i. El consentimiento explícito de los trabajadores resulta prescindible para la implementación de sistemas de videovigilancia en el ámbito laboral, dado que su base y su legitimación jurídica se fundamenta en la propia relación contractual de trabajo

y en las facultades que el ordenamiento jurídico reconoce al empleador en el ejercicio del poder de dirección y control de la actividad laboral en el artículo 20.3 del ET.

ii. De conformidad con los principios rectores del RGPD, en particular en principio de minimización de datos recogido en su artículo 5.1.c), el tratamiento de datos personales debe ajustarse a los criterios de adecuación, pertinencia y limitación, garantizando que la recopilación y el uso de información se restrinja a los estrictamente necesario para la finalidad legítima perseguida.

En el ámbito de la videovigilancia laboral ello implica que estos sistemas únicamente podrán ser implementados cuando no existan medios alternativos menos intrusivos que permitan alcanzar el mismo objetivo sin comprometer de manera desproporcionada a la privacidad de los trabajadores.

En esta línea la AEPD ha interpretado que la aplicación del principio de minimización impone una serie de limitaciones adicionales, entre las cuales se encuentran la obligación de restringir el número de dispositivos de captación de imágenes a aquellos que resulten imprescindibles para la finalidad de vigilancia establecida y la necesidad de realizar un análisis previo de los requisitos técnicos de los equipos utilizados. En este sentido el empleo de sistemas con capacidad de zoom, grabación en 360º, denominadas "cámaras domo" puede implicar un riesgo para la proporcionalidad, el tratamiento y, en consecuencia, vulnerar el principio de minimización, lo que exige que al responsable del tratamiento la adopción de medidas preventivas para garantizar la adecuación del sistema a los estándares normativos vigentes.

iii. La obligación del empleador de informar a las personas trabajadoras sobre la implementación de sistemas de videovigilancia en el centro de trabajo. El tratamiento de imágenes obtenidas a través de cámaras con fines de videovigilancia para el control empresarial deberá realizarse en el marco de la legalidad vigente y respetando los límites impuestos al empleador, siendo este que el empleador debe informar a los trabajadores (o a los representantes de los trabajadores, en su caso) con carácter previo, de manera expresa, clara y concisa sobre la adopción de esta medida (artículo 89.1 de la LOPDGDD).

El principio de transparencia, consagrado en el RGPD, también refuerza esta obligación de información, garantizando que los trabajadores sean debidamente advertidos de la instalación y finalidad de los dispositivos de videovigilancia, permitiéndoles ejercer así sus derechos en materia de protección de datos. Es por

ello por lo que cualquier incumplimiento de este deber informativo podría derivar en la en la ilicitud del tratamiento de datos, con las responsabilidades administrativas y legales correspondientes.

iv. El artículo 89.1 de la LOPDGDD establece una excepción en la obligación general de informar de manera previa y expresa a los trabajadores sobre la instalación de sistemas de videovigilancia. En términos jurídicos, esta disposición dispone que, cuando las cámaras capten de forma flagrante la comisión de un acto ilícito por parte del trabajador se considerara cumplido el deber de informativo por parte de la empresa, siempre que se haya colocado un dispositivo informativo visible que indique la existencia del sistema de videovigilancia.

Este artículo remite también al artículo 22.4, el cual establece los requisitos mínimos que deben cumplir los dispositivos informativos, en los que debe constar, de manera obligatoria: la existencia del sistema de videovigilancia, la identidad del responsable o encargado de tratamiento, quien será el responsable de la gestión y operación de las cámaras y la información relativa al ejercicio de los derechos de los trabajadores en materia de protección de datos, en cumplimiento con la normativa aplicable.

En consecuencia, el empleador no está obligado a informar individualmente a cada trabajador cuando se haya captado un acto ilícito, siempre que existan los carteles informativos correspondientes en lugares visibles. Esta exención está sujeta al cumplimiento de los principios de proporcionalidad y minimización de datos del RGPD. Así el trabajador que haya sido grabado cometiendo una infracción no podrá alegar desconocimiento de la existencia del sistema de videovigilancia si dichos carteles informativos estaban debidamente instalados y eran accesibles para todos los empleados.

v. El articulo 89.2 de la LOPDGDD establece una prohibición expresa respecto a la instalación de sistemas de videovigilancia en aquellos espacios destinados al descanso o esparcimiento de las personas trabajadoras, tales como vestuarios, comedores, aseos y análogos. Esta restricción encuentra su fundamento en la garantía del derecho a la intimidad reconocido en el artículo 18.1 de la CE y en el artículo 8 del CEDH.

vi. En lo que concierne a la supresión de datos, el artículo 22.3 de la LOPDGDD dispone que, en condiciones generales, las imágenes captadas mediante videovigilancia deberán ser eliminadas transcurrido un mes desde su registro. Se contempla una excepción para aquellos supuestos en que resulte imperativo conservar la información con el objeto de acreditar la comisión de conductas que

puedan comprometer la integridad de las personas o la seguridad de bienes e instalaciones. En tales situaciones excepcionales, se estipula que las grabaciones deberán ser remitidas s la autoridad competente en un plazo máximo de setenta y dos horas desde que se tenga constancia de la existencia del registro.

Es por todo ello que la videovigilancia laboral debe ejercerse de acuerdo con los principios de legalidad, proporcionalidad y trasparencia, respetando los derechos fundamentales a la intimidad y a la protección de datos. Su implementación exige una justificación legitima, información clara a los trabajadores y medias que eviten intromisiones desproporcionadas, garantizando de esta forma un equilibrio entre los intereses legítimos del empresario y la dignidad de las personas trabajadoras.

2.7.3 Geolocalización

El uso de dispositivos de geolocalización en el ámbito laboral ha sido objeto de un exhaustivo análisis doctrinal debido a la incidencia que tiene en la colisión de los derechos fundamentales del trabajador y las facultades empresariales de organización y control. Este sistema de control empresarial viene regulado en el RGPD, el contexto normativo europeo, donde establece los principios rectores para el tratamiento de datos personales, y de manera complementaria, a nivel nacional, la LOPDGDD, en su artículo 90 delimita las condiciones bajo las cuales los empleadores pueden recurrir a la geolocalización, imponiendo la obligación de informar de forma clara, expresa e inequívoca a los trabajadores sobre su implementación, finalidad y alcance.

Según la RAE entendemos la geolocalización como *"acción y efecto de geolocalizar"* entendiendo como geolocalizar la *"determinación de la ubicación geográfica de alguien o de algo valiéndose de medios técnicos avanzados, como el GPS"*.

Además la AEPD ha determinado que los datos obtenidos a través de la geolocalización constituyen información de carácter personal en la medida que permiten la identificación de los empleados mediante la recopilación de patrones de desplazamiento y localización en tiempo real.

Dentro del plano normativo, el artículo 90 de la LOPDGDD establece que el empleador tiene la facultad de tratar con los datos obtenidos mediante geolocalización para el ejercicio de funciones de control de la actividad laboral, pero dicha potestad está supeditada a que se respeten los principios de necesidad, idoneidad y proporcionalidad. De este modo la recopilación de datos de localización solo podrá justificarse cuando sea indispensable para la

organización del trabajo, la optimización de recursos o la seguridad del propio trabajador y de los bienes empresariales, pero no cuando su único propósito sea la fiscalización generalizada del cumplimiento de la jornada laboral sin justificación suficiente.

En este sentido, la Sentencia del Tribunal Superior de Justicia de Asturias de 27 de diciembre de 2018 (Rec. 2241/2017) declaró lícito el uso del GPS en vehículos asignados a trabajadores móviles cuya actividad implicaba desplazamientos constantes, al considerar que la medida respondía a una necesidad operativa de la empresa y se aplicaba exclusivamente dentro del horario de trabajo.

Valle Muñoz (2021) destaca que la geolocalización del trabajador a través de dispositivos GPS constituye un instrumento de control empresarial que puede ser utilizado como medio de prueba en el ámbito judicial. Sin embargo, su validez probatoria está condicionada al respeto de los derechos fundamentales del trabajador tal y como se dispone en el artículo 11.1 de la Ley Orgánica del Poder Judicial (en adelante LOPJ) que establece que *"no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales."*

En el contexto del derecho laboral, la geolocalización no solo debe cumplir con las exigencias de trasparencia e información, sino que también debe evitar la vulneración del derecho a la desconexión digital del trabajador. La utilización de sistemas de posicionamiento durante tiempos de descanso o fuera del horario laboral constituye una intromisión legitima en la vida privada del empleado, a menos que exista un interés empresarial de peso que justifique la medida siempre que se garantice su proporcionalidad (Kahale Carrillo, 2021)

A este respecto, Aguilera Izquierdo (2020) subraya que la implementación de sistemas de geolocalización en el ámbito laboral debe someterse a un riguroso escrutinio jurídico, no solo en lo que respecta al cumplimiento del marco normativo vigente en materia de protección de datos, sino también en relación con los principios constitucionales que limitan la injerencia del empleador en la esfera privada del trabajador.

El Tribunal Superior de Justicia de Madrid (en adelante TSJ) reforzó esta interpretación al señalar que el empleo de sistemas de geolocalización en vehículos corporativos, si bien puede resultar justificado como medida de supervisión del desempeño laboral, no puede derivar en un control absoluto y permanente de la actividad del trabajador, ya que ello supondría una intromisión desproporcionada en su derecho a la intimidad personal y familiar, reconocido en el artículo 18 de la CE. (Rec. 1952/2013)

Asimismo, la doctrina judicial ha puesto de manifiesto que la información recabada mediante estos sistemas no puede ser utilizada de manera indiscriminada para evaluar el comportamiento del trabajador fuera de su jornada laboral, pues ello vulneraría el derecho a la desconexión digital y a la separación entre la vida profesional y personal (STSJ de Andalucía, 19 de octubre de 2017, Rec. 1149/2017).

Por otro lado, en relación con la geolocalización fuera del horario laboral, la doctrina judicial ha sido contundente al señalar que la continuidad del rastreo del trabajador una vez finalizada la jornada laboral supone una vulneración de sus derechos fundamentales.

En este sentido, el Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes recomienda que los dispositivos utilizados por los empleados cuenten con una opción de desactivación durante su tiempo de descanso, de modo que se evite un control permanente que trascienda los límites del poder de dirección del empresario (AEPD, 2021)

Finalmente, la cuestión del consentimiento del trabajador ha sido objeto de debate en el ámbito jurisprudencial. Si bien en determinadas circunstancias el consentimiento no es un requisito indispensable para la instalación de sistemas de geolocalización (por encontrarse justificado en el cumplimiento de trabajo y en el interés legítimo del empleador), la doctrina judicial ha determinado que, cuando estos dispositivos permiten la monitorización continua del trabajador o se utilizan con fines distintos a los inicialmente previstos, el consentimiento expreso se convierte en un requisito esencial. Así lo recoge la Sentencia del Tribunal Superior de Justicia de Andalucía de 19 de octubre de 2017 (Rec. 1149/2017), que declaró nulo el despido de una trabajadora cuya conducta fuera del horario laboral fue monitorizada mediante GPS sin su conocimiento ni autorización expresa. Es por ello por lo que se debe enfatizar en la necesidad de diferenciar entre el uso legítimo del control empresarial y las intromisiones arbitrarias que comprometan los derechos fundamentales del trabajador.

2.7.4 Datos biométricos

El uso de tecnologías basadas en los datos biométricos en el ámbito laboral constituye una creciente e intensa reflexión jurídica, además de un conflicto entre el poder de dirección y control del empleador, y los derechos fundamentales del trabajador. Se entiende por datos biométricos aquellos "*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*" (artículo 4.14 del RGPD).

Las tecnologías biométricas en el ámbito laboral suelen utilizarse como sistemas con finalidad de control de acceso a las instalaciones o la verificación de la identidad de los trabajadores para el registro de la jornada laboral. No obstante, es importante precisar que no todo tratamiento biométrico es automáticamente calificado como tratamiento de categorías especiales de datos. El artículo 9.1 del RGPD precisa que únicamente se consideran categorías especiales aquellos datos biométricos destinados a identificar de manera unívoca a una persona física.

Por lo tanto, solo cuando exista un tratamiento técnico especifico orientado a esa identificación única, se activarán las salvaguardas más intensas. (AEPD, 2021).

Es fundamental en este caso diferenciar entre dos supuestos de tratamiento: la identificación o la verificación o autentificación biométrica.

La identificación consiste en determinar la identidad de un individuo entre un conjunto de personas, mientras que la verificación se limita a confirmar la identidad declarada por una persona, comparando los datos con la información previamente asociada a esa identidad. (AEPD, 2021)

Esta diferenciación, reconocida en el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 y posteriormente recogida en el Convenio 108+ del Consejo de Europa y en el Libro Blanco sobre inteligencia artificial de la Comisión Europea, es relevante porque solo los tratamientos dirigidos a la identificación caen habitualmente dentro de la categoría especial de datos (artículo 4 del RGPD).

La AEPD recomienda priorizar los sistemas de verificación/autenticación, sugiriendo que los datos biométricos se almacenen en plantillas cifradas, conservadas en soportes controlados directamente por las personas trabajadoras (como tarjetas inteligentes). Por ejemplo, en los sistemas de control de acceso basados en biometría, se puede requerir tanto la presentación de una tarjeta como la lectura de una huella dactilar, de modo que ambos elementos coincidan y se valide el acceso (AEPD, 2021).

El tratamiento de estos datos podría excluirse de la prohibición general en virtud del artículo 9.2.b del RGPD, cuando sea necesario para cumplir con las obligaciones laborales o de Seguridad Social, siempre que exista respaldo normativo suficiente, como un convenio colectivo o normativa nacional. A este respecto, el artículo 20.3 del ET habilita al empresario a adoptar medidas de control, siempre respetando la dignidad del trabajador.

Sea cual sea la modalidad (identificación o verificación), el tratamiento debe cumplir estrictamente las garantías previstas en la normativa. (AEPD, 2021)

Entre ellas destacan:

- La obligación de informar adecuadamente al trabajador;
- La incorporación de medidas de protección de datos desde la fase de diseño del sistema;
- El almacenamiento preferente en dispositivos personales con claves de cifrado específicas;
- La restricción de reutilización de los datos para finalidades distintas;
- La eliminación de los datos cuando dejen de ser necesarios.

Además, si se opta por un sistema de identificación, resultará obligatorio realizar una evaluación de impacto. La evaluación de impacto se trata de un instrumento preventivo que debe realizar previamente el responsable de tratamiento cuando una actividad de tratamiento de datos personales pueda suponer un riesgo muy elevado para los derechos y libertades de las personas, haciendo especial referencia a los supuestos de tratamiento de datos automatizado o de categorías especiales de datos. Esta evaluación de impacto viene recogida en el artículo 35 del RGPD y consiste en realizar un análisis exhaustivo donde debe detallarse: las operaciones previstas, su finalidad, la necesidad y proporcionalidad del tratamiento, los riesgos detectados y las medidas técnicas y organizativas adoptadas con el objetivo de minimizar dichos riesgos, garantizando el buen cumplimiento del RGPD.

Por último, el artículo 91 de la LOPDGDD permite que los convenios colectivos introduzcan garantías adicionales en materia de protección de datos en el ámbito laboral.

Desde un punto de vista jurisprudencial, la Sentencia del Tribunal Supremo en adelante (STS) de 25 de febrero de 2020 validó el uso de sistemas biométricos para el registro horario siempre que se respetaran los principios de necesidad, idoneidad y proporcionalidad.

También la STC 39/2016 reconoció la licitud del uso de huellas dactilares para el control de acceso a las instalaciones y centros de trabajo, remarcando la importancia del equilibrio entre el control empresarial y los derechos fundamentales.

Sin embargo, en la actualidad conforme a lo establecido en la guía sobre tratamientos de control de presencia mediante sistemas biométricos (AEPD, 2023), el tratamiento de datos biométricos con fines de registro de jornada laboral resulta, con carácter general, incompatible con la normativa vigente de protección de datos, al carecer de una "autorización suficientemente específica" en el ordenamiento jurídico español.

Tal y como recoge la guía, *"en la actual normativa legal española no se contiene autorización suficientemente específica alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo"*.

Asimismo, el consentimiento de la persona trabajadora no resulta válido en este contexto, dada la existencia de un "claro desequilibrio de poder" en la relación laboral, lo que impide que pueda prestarse libremente conforme al artículo 9.2.a) del RGPD.

En consecuencia, la utilización de sistemas biométricos para el fichaje laboral no resulta lícita, salvo en supuestos excepcionales que acrediten de forma estricta la necesidad, idoneidad y proporcionalidad del tratamiento conforme a los artículos 5.1.c), 6.1 y 9.2 del RGPD

2.7.5 Control de falta de asistencia por enfermedad o accidente

Otro de los aspectos relevantes relativos a la facultad de control empresarial sobre los trabajadores, es como el ET faculta a las empresas a realizar controles médicos a aquellas personas trabajadoras que se ausenten del trabajo por motivos de enfermedad o accidente. Esta facultad viene recogida en el artículo 20.4 del ET donde se establece que *"el empresario podrá verificar el estado de salud del trabajador, para justificar sus faltas de asistencia al trabajo, mediante reconocimientos a cargo del personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones"*

No obstante, el control de falta de asistencia por enfermedad o accidente no se puede comparar con las normas que regulan la vigilancia de la salud relativas a la prevención de riesgos (AEPD, 2021).

Cabe destacar como características de los controles de absentismo por enfermedad o accidente las siguientes (AEPD, 2021)

- La comprobación del estado de salud del trabajador implica el tratamiento de información relativa a la salud, y es por ello por lo que se enmarca en las denominadas categorías especiales de datos

- El fundamento jurídico que permite este tratamiento se justifica en el propio contrato de trabajo, por lo que no resulta necesario que el trabajador otorgue su consentimiento, en relación además con las sanciones que pueden derivarse si se niega a someterse al examen correspondiente.
- La empresa no está autorizada para acceder a información clínica detallada, pero si para conocer la valoración final que determine si la persona trabajadora esta apta o no para reincorporarse a su puesto de trabajo.
- Registrar sistemáticamente información médica con el único propósito de vigilar el absentismo puede considerarse una medida excesiva, que vulnera el principio de minimización de datos y de proporcionalidad.

Es importante hacer referencia a casos en los que este control se realiza mediante la contratación de un servicio externo, ya que además del deber de cumplimiento del encargado de tratamiento, dicho servicio debe atenerse a ciertas peculiaridades (AEPD, 2021)

- El deber de información a la persona trabajadora debe ser muy preciso, indicando aquí que se trata de un control laboral.
- En el supuesto caso en el que los datos de la persona trabajadora se incorporen a una historia clínica, pasara el prestador de este servicio externo a considerarse también responsable de tratamiento.

En estos casos donde las empresas contratan servicios externos para llevar a cabo el control de absentismo, sí que se consideran legitimados para elaborar informes estadísticos sobre el índice de absentismo y las causas que lo motivan, siempre y cuando no contengas datos personales. Estos datos deben ser disociados, no permitiéndose de esta manera que las personas trabajadoras sean identificadas. (AEPD, 2021)

2.7.6 Detectives privados

El sistema de control mediante detectives privados se encuentra regulado en la Ley 5/2014, de 4 de abril, de seguridad privada.

Del mismo modo que los empleadores están facultados para implementar diferentes medias y sistemas de control, también podrán emplear sistemas de investigación privada a través de detectives privados, siempre y cuando se observen los siguientes requisitos (AEPD, 2021)

- La adopción de esta medida debe superar el test de proporcionalidad, pudiéndose aplicar únicamente cuando no existan alternativas menos intrusivas para alcanzar la misma finalidad.

- En ningún supuesto podrán dirigirse actuaciones de investigación hacia la esfera privada del trabajador, entendiéndose como tal su domicilio u otros lugares específicos de su vida privada, cuando ello pueda suponer la vulneración al derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones o a la protección de datos, según lo recogido en el artículo 48.3 de la Ley 5/2014, de 4 de abril, de seguridad privada.

En cuanto a los informes emitidos por los detectives privados, estos deberán ajustarse a una serie de disposiciones recogidas en el artículo 49 de la Ley 5/2014, de 4 de abril, de seguridad privada:

- La información incorporada a dicho informe deberá ceñirse exclusivamente al objeto y finalidad de la investigación para la que fue contratada. Queda expresamente prohibido la inclusión de información, referencias o datos que se hayan podido averiguar incidentalmente (especialmente datos de carácter personal) que sean innecesarios o que no estén directamente relacionados con el interés legítimo de dicha contratación
- Dicho informe será puesto a disposición del cliente, quien, en su caso, será el encargado de remitirlo a las autoridades policiales correspondientes para su posterior inspección.
- Los informes deberán ser archivados por un periodo mínimo de 3 años. Por su parte, las imágenes y los sonidos obtenidos durante el desarrollo de la investigación deberán ser destruidos a los tres años, salvo que resulten necesarios para procedimientos judiciales, investigaciones policiales o procedimientos sancionadores.
- Todos los informes de investigación tendrán carácter estrictamente confidencial, y su contenido solo podrá ser facilitado al cliente o en su caso de las administraciones correspondientes, por lo que se consideran de carácter reservado.

En cualquiera de los casos, este tipo de medida deberá ser respaldada por las obligaciones establecidas en el RGPD y la LOPDGDD y especialmente en la Ley 5/2014, de 4 de abril, de seguridad privada

3. JURISPRUDENCIA RELEVANTE

- STS 4902/2024 - ECLI:ES:TS:2024:4902 STS SALA DE LO CONTENCIOSO

El Tribunal Supremo, Sala de lo Contencioso-Administrativo, resuelve un recurso de casación interpuesto por el Ayuntamiento de Algemesí, contra una sentencia de la Audiencia Nacional, la cual confirmó la resolución de la AEPD en la que se declaraba que el Ayuntamiento de Algemesí había vulnerado el derecho fundamental a la protección de datos personales.

Los hechos acreditativos de esta sentencia son los siguientes:

- Una funcionaria del Ayuntamiento de Algemesí fue objeto de un expediente disciplinario
- Se le acusa de utilizar la impresora del Ayuntamiento para llevar a cabo actividades personales, ajenas a su trabajo diario y a su función pública
- El 26 de febrero de 2018, sin previo aviso ni consentimiento, y sin intervención judicial ni procedimiento formalizado, se accede de forma remota a su ordenador de trabajo por parte del departamento de informática, por orden directa de la alcaldesa del Ayuntamiento.
- El informático vuelca en un DVD no cifrado varias carpetas personales y profesionales, que posteriormente fueron entregadas a la alcaldesa y además utilizadas como base probatoria en el expediente disciplinario.
- Dentro de los datos del DVD se encontraban declaraciones de la renta, documentos bancarios, contratos, documentos médicos…muchos de ellos considerados como datos especialmente protegidos.

A continuación, se exponen los fundamentos jurídicos clave de esta sentencia:

- Infracción del consentimiento (artículo 6.1 de la LOPD, actuales artículos 6 y 8 de la LOPDGDD), ya que el tratamiento de datos personales de la trabajadora se llevó a cabo sin su consentimiento, y sin una base jurídica suficiente.
- Datos especialmente protegidos (artículo 9 RGPD): la copia contenía datos sensibles relativos a la salud y datos financieros, sin delimitación de la finalidad de dicho tratamiento y sin medidas de minimización ni garantías de confidencialidad (artículos 5.1 y 32 del RGPD)
- Privacidad en el entorno laboral público: el Ayuntamiento de Algemesí justificó su intervención en la "titularidad pública" de los equipos informáticos como base jurídica para justificar el acceso.

- Hacemos referencia en este apartado a la Doctrina Barbulescu, ya que el TS afirma que esta doctrina del TEDH también se debe proyectar, dado que el derecho fundamental de protección de datos no desaparece por el tipo de empleador, y que las garantías constitucionales son también aplicables a las Administraciones públicas.

Por todo ello finalmente el TS confirmo la infracción por parte del Ayuntamiento, por vulnerar los derechos de consentimiento, medidas de seguridad, protección de datos y el artículo 18 de la CE.

- ATS ATS 13600/2022 - ECLI:ES:TS:2022:13600A STS SALA DE LO SOCIAL

En esta sentencia el TS rechaza el recurso de casación para la unificación de doctrina interpuesto por la empresa Transportes J. Carrión S.A.U contra la sentencia del TSJ de Cataluña, el cual declaro improcedente el despido de un trabajador. La empresa justifico la sanción impuesta en base a datos de geolocalización obtenidos del vehículo de empresa asignado al trabajador. Sin embargo, no acreditaron haber informado al trabajador un a sus representantes sobre el uso de dichos dispositivos de geolocalización.

Los hechos acreditativos de esta sentencia son los siguientes:

- El trabajador despedido desempeñaba funciones como conductor mecánico desde el año 2004.
- En octubre de 2019 la empresa detecto mediante sistemas de geolocalización paradas anómalas en sus rutas laborales.
- Se comprobó posteriormente que vendía pellets presuntamente sustraídos a terceros.
- Se impuso un despido disciplinario por transgresión de la buena fe contractual.
- Los dispositivos de geolocalización se encontraban instalados tanto en el camión como en el remolque, pero no se había informado al trabajador de dicha instalación.

A continuación, se exponen los fundamentos jurídicos clave de esta sentencia:

- El artículo 219 de la Ley Reguladora de la Jurisdicción social exige la existencia de contradicción efectiva entre la sentencia recurrida y la de contraste.
- El tribunal rechaza la existencia de identidad sustancial entre ambas resoluciones comparadas, ya que en la sentencia de contraste el trabajador si estaba informado del sistema de geolocalización, mientras que en el caso actual no se acredito ningún tipo de información previa al trabajador, incumpliendo por lo tanto lo exigido en el artículo 90 de la LOPDGDD

- La prueba resulto ilícita al considerar que la empresa vulnero el derecho del trabajador a la protección de datos personales (artículo 18.4 de la CE)
- El incumplimiento de los principios de información, transparencia y finalidad, conforme a los establecido en el RGPD y la LOPDGDD

Por todo ello finalmente el TS no admite el recurso por falta de contradicción doctrinal. La sentencia del TSJ de Cataluña, que declaró improcedente el despido por prueba ilícita, quedó firme e intacta.

- STS 1054/2025 - ECLI:ES:TS:2025:1054 STS SALA DE LO CIVIL

Esta sentencia aborda un recurso de casación por intromisión ilegítima en el derecho a la intimidad. Esta sentencia tiene como origen una demanda interpuesta por Dª Marí Jose contra Vialegis Abogados, S.L.P, debido a la difusión de datos personales contenidos en una demanda laboral en una carpeta compartida de la empresa. El Juzgado de Primera Instancia y la Audiencia Provincial desestimaron la demanda.

Los hechos acreditativos de esta sentencia son los siguientes:

- Dª Marí Jose demando a la empresa Vialegis Abogados, S.L.P por modificación sustancial de las condiciones de trabajo en enero de 2020. En la demanda se incluían datos personales y sensibles (sueldo, procesos de incapacidad temporal, ansiedad por acoso laboral…)
- La demanda fue escaneada y almacenada con el nombre "Demanda Marí Jose" en una carpeta común del despacho, a la que todos los trabajadores tenían acceso sin restricciones.
- Una excompañera de trabajo accedió al documento en la carpeta compartida a pesar de no estar autorizada para ello.
- La Audiencia Provincial reconoció la falta de protección de la carpeta compartida constituía una brecha de seguridad.
- No se aprobó que la empresa demandada hubiera adoptado medias técnicas y organizativas adecuadas para garantizar la seguridad de los datos y evitar accesos no autorizados.
- La abogada de la demandada que escaneo el documento afirmo que el archivo solo estuvo en la carpeta común el tiempo necesario y luego fue eliminado.

A continuación, se exponen los fundamentos jurídicos clave de esta sentencia:

- Articulo 5.1 del RGPD, se destaca que Vialegis Abogados, S.L.P debia cumplir con los principios de minimización, confidencialidad y seguridad en el tratamiento de los datos de la persona demandante.
- Artículo 5.2 del RGPD, ya que el responsable del tratamiento debe ser capaz de demostrar responsabilidad proactiva y el cumplimiento de esta.
- Artículo 24 del RGPD ya que en la sentencia se hace referencia a la falta de adopción de medidas técnicas y organizativas apropiadas por parte de la empresa en materia de protección de datos.

Por todo ello finalmente el TS estima el recurso de casación de Dª Marí Jose, revoca las sentencias de instancias anteriores y declara que Vialegis Abogados, S.L.P incurrió en intromisión ilegítima en el derecho a la intimidad de la demandante. Se condena a la demandada a pagar 3.000€ como indemnización del daño moral y a abstenerse de realizar actos semejantes en el futuro.

- SENTENCIA 29/2013. RECURSO DE AMPARO STC

En esta sentencia se hace referencia a un trabajador, cuya sanción disciplinaria se basó en imágenes de videovigilancia. El Tribunal Constitucional considera que la utilización de estas imágenes con fines de supervisión laboral, sin haber informado previamente al trabajador de dicha finalidad, vulnera el derecho a la protección de datos de carácter personal. Y aunque la videovigilancia fuera conocida, su uso para un propósito diferente al inicialmente justificado requería una información específica al afectado.

Los hechos acreditativos de esta sentencia son los siguientes:

- La universidad de Sevilla tenía instaladas cámaras de videovigilancia en todo el recinto universitario.
- No se informó al trabajador de que la finalidad de la videovigilancia incluía la supervisión del trabajo. La sentencia menciona (pág. 27) *"Utilización de imágenes captadas por las cámaras de videovigilancia instaladas en el recinto universitario para una finalidad, la supervisión laboral, de la que no se informó al trabajador".*
- La Universidad de Sevilla impuso una sanción disciplinaria al trabajador, basándose en las imágenes obtenidas de videovigilancia.

A continuación, se exponen los fundamentos jurídicos clave de esta sentencia:

- Deber de información previa sobre la finalidad del tratamiento de datos: el Tribunal reitera la importancia del deber de informar al interesado sobre la finalidad àra la cual sus datos van a ser utilizados. La mera existencia de cámaras o el conocimiento general de la videovigilancia no exime de informar sobre los usos específicos de los datos personales.
- Finalidad especifica y principio de proporcionalidad: aunque la videovigilancia por motivos de seguridad pueda ser legítima, si su uso se destina a un fin diferente, como el control laboral, exige una justificación y una información adecuada. Esta sentencia aplica el principio de proporcionalidad, donde se considera que no es proporcional si no se cumple con el requisito de información.

Por todo ello finalmente el TC decidió otorgar el amparo solicitado por D. Adolfo Tomás Fraile Nieto. Como consecuencia se declara la vulneración de du derecho fundamental a la protección de datos de carácter personal, y por ende se anularon las sentencias previas del Juzgado de lo Social y el TDJ de Andalucía, así como la resolución sancionadora de la Universidad de Sevilla que impuso la sanción disciplinaria al recurrente.

4. CONCLUSIONES

Este trabajo de investigación ha explorado un tema de gran importancia en nuestra actualidad: como las empresas pueden supervisar el trabajo de sus empleados sin invadir sus derechos más básicos, como la privacidad o la protección de sus datos personales. La idea inicial o hipótesis era la siguiente: si las empresas actúan con sensatez y cumplen las reglas, es posible encontrar un punto medio donde se respeten tanto los intereses de la empresa como los derechos de los trabajadores. Los resultados de este Trabajo de Fin de Grado confirman esta idea. Hemos confirmado que ese equilibrio no solo es posible, sino que es la única forma válida y legal para que una empresa controle a sus empleados hoy en día.

Cuando una empresa ejerce su poder de control de forma adecuada, es decir, respetando los principios de proporcionalidad, necesidad y equilibrio, este control no solo es legítimo, sino que ayuda a la empresa a llevar un correcto funcionamiento sin pisar la dignidad del empleado. La jurisprudencia insiste en que cualquier medida debe ser muy bien meditada por las empresas, deben servir para algo útil y no debe haber una forma menos intrusiva de conseguir este fin. De esta forma el beneficio para la empresa debe ser mayor que las "molestias" que los sistemas de control puedan ocasionar en los empleados. Si una medida de control cumple con estos requisitos, entonces es válida.

Un punto crucial que destacar es la "minimización de datos" esto quiere decir que las empresas solo deben recoger y tratar la información del trabajador que sea estrictamente necesaria para el fin que buscan. Si se recoge más información de la necesaria, o si esa información se utiliza para un fin diferente por el cual no se puso en aviso al trabajador, no solo se estarían incumpliendo las leyes de protección de datos, sino que se invadirían los derechos fundamentales de la persona.

Además, es fundamental "la limitación de la finalidad". Las empresas deben dejar muy claro desde el principio para qué van a utilizar la información o los sistemas de control. Si luego dicha información es utilizada para un fin diferente del que inicialmente se estableció, sin el permiso del trabajador o sin una ley que lo autorice, se estaría actuando de forma incorrecta y abusando del poder.

La segunda parte de la hipótesis también se ha confirmado con rotundidad: si la empresa no informa bien o utiliza sus herramientas de control de forma exagerada, es altamente probable que vulnere los derechos de los trabajadores y tenga que asumir consecuencias legales. La falta de transparencia es un error grave de las empresas. El trabajador tiene derecho a saber qué información se recoge sobre él y sobre todo para que se está utilizando. Si no se le

informa, el trabajador no puede defenderse ni saber si sus derechos están siendo respetados, dejando a la empresa en una situación muy vulnerable ante una posible demanda.

El "uso excesivo" de los sistemas de control empresarial no solo se refiere a vigilar durante demasiado tiempo o en demasiados lugares, sino usar tecnologías muy invasivas sin una razón de peso que lo justifique. Instalar sistemas de vigilancia muy avanzados sin que haya motivo real o que la medida sea más grave que el problema que se quiere resolver llevará a que las pruebas obtenidas sean invalidas y que se declare la violación de derechos de los trabajadores como la intimidad o la privacidad de los trabajadores.

Este trabajo concluye que las empresas si pueden ejercer su facultad de control empresarial, al mismo tiempo que respetan los derechos de los trabajadores. La consecución de este equilibrio se articula en la aplicación consciente y transparente de los principios de proporcionalidad, minimización de datos y limitación de la finalidad. Aquellas organizaciones que integren y promuevan activamente las buenas prácticas, no solo mitigaran eficazmente los riesgos de contingencias legales y responsabilidades sancionadoras, sino que, además, de forma inherente se fomentara un clima organizacional fundamentado en el respeto recíproco.

5. BIBLIOGRAFÍA

- Agencia Española de Protección de Datos (AEPD). (2021). *Guía sobre el uso de videocámaras para seguridad y otras finalidades*. https://www.aepd.es/guias/guia-videovigilancia.pdf
- Agencia Española de Protección de Datos (AEPD). (2023). *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*
- Agencia Española de Protección de Datos (AEPD). (2021). *Informe 0613/2009 sobre geolocalización y protección de datos en el ámbito laboral.*
- Agencia Española de Protección de Datos (AEPD). (2021). *La protección de datos en las relaciones laborales*. https://www.aepd.es/guias/la-proteccion-de-datos-en-las-relaciones-laborales.pdf
- Agencia Española de Protección de Datos (AEPD). *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a la protección de datos*. https://www.aepd.es/documento/listas-dpia-es-35-4.pdf
- Aguilera Izquierdo, R. (2020). El derecho a la protección de datos en el ámbito laboral: Los sistemas de videovigilancia y geolocalización. *Revista de Trabajo y Seguridad Social. CEF*, (442), 93-134.
- Constitución Española. («BOE» núm. 311, de 29 de diciembre de 1978). https://www.boe.es/buscar/pdf/1978/BOE-A-1978-31229-consolidado.pdf
- Convenio Europeo de Derechos Humanos. (1950, 4 de noviembre). (Entrada en vigor: 3 de septiembre de 1953). https://www.echr.coe.int/documents/d/echr/convention_spa
- García Hernández, A. (2022). Responsabilidad civil de encargados y responsables del tratamiento de datos en el Reglamento UE de protección de datos. *Revista CESCO de Derecho de Consumo*, (41), 133-153. https://dialnet.unirioja.es/servlet/articulo?codigo=8474083
- Grupo de Trabajo del Artículo 29. (2005). *Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido*. https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf
- Grupo de Trabajo del Artículo 29. (2011). *Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_es.pdf
- Grupo de Trabajo del Artículo 29. (2012). *Dictamen 3/2012 sobre evolución de tecnologías biométricas*. https://www.aepd.es/documento/wp193_es.pdf

- Kahale Carrillo, D. T. (2021). La geolocalización como medio de control del trabajador. *Temas Laborales*, (157), 141-166.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. («BOE» núm. 294, de 06 de diciembre de 2018). https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf
- Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza. (2020). Comisión Europea. https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_es?filename=commission-white-paper-artificial-intelligence-feb2020_es.pdf
- Orellana Cano, A. M. (2019). *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores.*
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. («BOE» núm. 255, de 24 de octubre de 2015). https://www.boe.es/buscar/pdf/2015/BOE-A-2015-11430-consolidado.pdf
- Tribunal Superior de Justicia de Andalucía. (2017). Sentencia Rec. 1149/2017.
- Tribunal Superior de Justicia de Asturias. (2018). Sentencia Rec. 2241/2017.
- Tribunal Superior de Justicia de Madrid. (2014). Sentencia Rec. 1952/2013.
- Tribunal Supremo de Madrid. Sala de lo Contencioso. Sentencia Rec. 6949/2022
- Tribunal Supremo de Madrid. Sala de lo Social. Sentencia Rec. 3256/2021
- Tribunal Supremo de Madrid. Sala de lo Civil. Sentencia Rec. 4109/2024
- Tribunal Constitucional. Sala Primera. Sentencia 29/2013.
- Valle Muñoz, F. A. (2021). Los dispositivos de geolocalización del trabajador como medio de prueba en el proceso laboral. *Ars Iuris Salmanticensis*, *9*, 29-55.