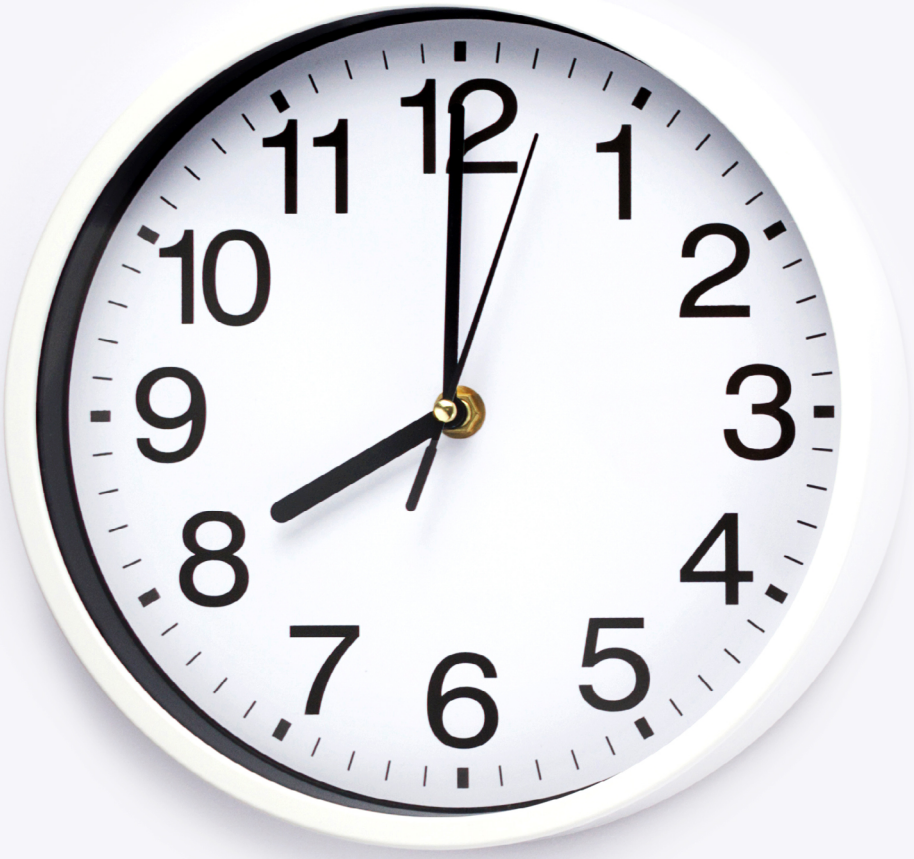


agencia española protección datos

La protección de datos en las relaciones laborales

Guía actualizada en
diciembre 2025

ÍNDICE

1. PRESENTACIÓN DE LA GUÍA

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, general de protección de datos (en adelante, RGPD) no se limita a reconocer el derecho a la protección de datos personales, sino que exige que cada Estado Miembro se dote de una infraestructura administrativa que permita proteger adecuadamente ese derecho. A tal fin, cada Estado Miembro debe contar con una autoridad de control que ejercerá las competencias y funciones relativas a la protección de datos personales, entre ellas la potestad sancionadora frente a incumplimientos en esta materia.

En concreto, el art. 57 del RGPD confiere a la autoridad de control funciones como:

- «Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento».

- «Promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones» en materia de protección de datos.

En España esa condición de autoridad de control, por lo que respecta al tratamiento de datos en el ámbito laboral privado, corresponde a la Agencia Española de Protección de Datos (en adelante, AEPD), que, desde hace décadas, ha publicado distintas guías para promover y clarificar la aplicación de la legislación de protección de datos. Uno de los principales objetivos de estas publicaciones ha sido ofrecer herramientas de ayuda a las organizaciones, públicas o privadas, para un adecuado cumplimiento de la legalidad vigente.

En este contexto, durante la vigencia de la regulación anterior se publicó una «Guía sobre protección de datos en las relaciones laborales», con el fin de examinar aspectos de la protección de datos que, o bien resultan fundamentales desde el punto de vista de la aplicación y el cumplimiento normativo, o bien planteaban dificultades de interpretación o aplicación práctica.

El nuevo marco normativo que configura el RGPD, junto con la posterior aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), ha introducido numerosos cambios en la regulación, que exigen una adaptación de la guía a esa nueva realidad legislativa. La LOPDGDD, por otro lado, incluye un Título X que reconoce un amplio conjunto de “derechos digitales” sobre los que, según su art. 2.1, la AEPD es competente para velar por los recogidos en los arts.89 al 94.

El propósito de la Agencia no consiste, exclusivamente, en resumir o estructurar el contenido de esas normas, sino en proporcionar una orientación de carácter práctico, no vinculante, que facilite a los responsables del tratamiento de datos personales y a las personas o entidades encargadas del tratamiento (en terminología del RGPD y en adelante, “encargados del tratamiento”) el cumplimiento de la legislación, con el apoyo de la experiencia atesorada por la AEPD a lo largo de los años.

La elaboración de este documento se ha realizado con la participación tanto del Ministerio del Trabajo y Economía Social como de organizaciones empresariales (CEOE y CEPYME) y sindicales (CCOO y UGT).

2. ASPECTOS GENERALES

1. CONCEPTO DE TRATAMIENTO DE DATOS PERSONALES

El art. 4.1 del RGPD considera **dato personal «toda información relativa a una persona física identificada o identificable»**.

A modo de ejemplo:

- Información que puede ser asociada a una persona física concreta: **nacimiento, matrimonio, domicilio**, etc.
- Información **numérica, alfabética, gráfica, fotográfica, acústica** o de cualquier otro tipo.
- Información sobre la **infancia**, sobre la **vida académica, profesional o laboral**, sobre los **hábitos de vida y consumo**, sobre las **relaciones personales** o sobre las **creencias religiosas e ideologías.**
- Nombre y apellidos, números de **identificación**, datos de **localización**, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social.
- También se consideran datos personales las **evaluaciones y apreciaciones** que hagan referencia a personas concretas.

El art. 9.1 del RGPD considera **categorías especiales de datos personales** aquellas que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física y los datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Con carácter general, el **tratamiento de categorías especiales de datos personales** está prohibido. Sin embargo, el art. 9.2 del RGPD admite su tratamiento cuando, entre otros supuestos, es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.

Ejemplo.

Tratamiento del dato de discapacidad de la persona trabajadora a efectos de reducciones o bonificaciones de cuotas a la Seguridad Social.

El derecho a la protección de datos ampara a los afectados frente al «tratamiento» de los mismos, que se define en el art. 4.2 del RGPD como **cualquier operación sobre datos personales**, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

La legislación de protección de datos **es de aplicación al tratamiento de datos efectuado por un empleador respecto de las personas trabajadoras**, sin perjuicio de que el art. 88 del RGPD permita que, mediante disposiciones legales o convenios colectivos, se establezcan «normas más específicas» con la finalidad de ofrecer una mejor y más adaptada protección del derecho a la protección de datos en el campo de las relaciones laborales.

No se considera tratamiento de datos sometido al RGPD y a la LOPDGDD el realizado en el ejercicio de **actividades exclusivamente personales o domésticas (art. 2.2.c) del RGPD)**.

2. BASES JURÍDICAS PARA EL TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales no puede realizarse por una razón de oportunidad, por la fácil obtención de estos o por si acaso en el futuro pudieran ser de utilidad, sino que exige que el responsable del tratamiento cuente con una «**base jurídica**» que le legitime para ello.

En el ámbito de las relaciones laborales, la **base jurídica principal** es la ejecución del contrato **de trabajo**, porque el consentimiento del afectado no es válido cuando se proporciona en un contexto de «**desequilibro claro entre el interesado y el responsable del tratamiento**», La posición de desequilibrio entre la empresa y la persona trabajadora exige extremar las cautelas y, en particular, el respeto a los principios de **proporcionalidad y de limitación de la finalidad**.

«Es muy poco probable que el consentimiento constituya una base jurídica para el tratamiento de datos en el trabajo, a no ser que los trabajadores puedan negarse sin consecuencias adversas […] Salvo en situaciones excepcionales, los empresarios tendrán que basarse en otro fundamento jurídico distinto del consentimiento, como la necesidad de tratar los datos para su interés legítimo. Sin embargo, un interés legítimo en sí mismo no es suficiente para primar sobre los derechos y libertades de los trabajadores» **(Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29[1]).**

Ejemplo:

"En efecto, de conformidad con la doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta con recordar que para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los

1 Grupo de trabajo sobre protección de datos del artículo 29 (GT29), Dictamen 02/2017 sobre el tratamiento de datos en el trabajo, WP 249, adoptado el 8 de junio de 2017. El Grupo de Trabajo se creó de conformidad con el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de dicha Directiva y en el artículo 15 de la Directiva 2002/58/CE. El Comité Europeo de Protección de Datos (CEPD), organismo independiente responsable de asegurar la consistente aplicación del RGPD, ha sucedido al GT29.

tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto) [SSTC 66/1995, de 8 de mayo, FJ 5; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero]" (STS 817/2017, de 2 de febrero, Sala de lo Social).

De este modo, el tratamiento de datos de las personas trabajadoras por parte del empleador es lícito, en primer lugar, **cuando sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales** (art. 6.1.b) RGPD).

La empresa podrá tratar datos como el nombre y los apellidos de las personas trabajadoras, su fecha de nacimiento, su sexo, su nacionalidad, su formación previa o cualesquiera otros imprescindibles para formalizar el contrato y ejecutar el trabajo.

En segundo lugar, el tratamiento de datos también es lícito «para el cumplimiento de una **obligación legal** aplicable al responsable del tratamiento» (art. 6.1.c) RGPD). Esta base jurídica permite el tratamiento de datos cuando sea necesario para cumplir las exigencias impuestas por la ley (por ejemplo, cotización a la Seguridad Social, obligaciones tributarias, registro de jornada, información y consulta con los representantes de las personas trabajadoras, etc.) o por un **convenio colectivo**.

Ejemplo:
Solicitud de la empresa a las personas trabajadoras de datos que acrediten que mantienen las autorizaciones necesarias para el desempeño de la actividad, como por ejemplo el permiso de conducir en caso de conductores.

En tercer lugar, también es base jurídica para el tratamiento de datos la satisfacción de **intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales (art. 6.1.f) RGPD). El Comité Europeo de Protección de Datos ha emitido la siguiente opinión sobre este punto:

«En caso de que un empresario pretenda invocar un interés legítimo [artículo 7, letra f)], la finalidad del tratamiento debe ser legítima; el método elegido o la tecnología específica deben ser necesarios, proporcionados y aplicados de la manera menos intrusiva posible, y el empresario deberá poder demostrar que se han adoptado las medidas adecuadas para garantizar un equilibrio con los derechos y libertades fundamentales de los trabajadores […] Estas limitación podrían: a) ser geográficas (por ejemplo, control únicamente en lugares específicos; debe prohibirse el control en zonas sensibles como lugares religiosos y, por ejemplo, zonas de aseos y salas de descanso), b) estar orientadas a datos (por ejemplo, los archivos electrónicos personales y las comunicaciones no deben ser controlados), y c) ser temporales (por ejemplo, muestreo en lugar de control continuo)» (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

Se presume que es necesario «para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero» el tratamiento de los **datos de contacto** y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos (art. 6.1.f) del RGPD y art. 19.1 de la LOPDGDD):

a) Que el tratamiento se refiera únicamente a los **datos necesarios** para su localización profesional, como el nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. No obstante, no se permite **el tratamiento de datos que no sean estrictamente necesarios** para cumplir esas finalidades, como sucedería, con el **número de DNI**.

> Esta base jurídica no se refiere a la relación entre el empleador y las personas trabajadoras, sino que, al tratamiento de datos de contacto, de carácter profesional, de una persona física por parte de un tercero, con el propósito de ponerla en contacto con una persona jurídica, lo que puede requerir la intermediación de esa persona física que actúa a modo de representante o de enlace.

b) Que la **finalidad del tratamiento** sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios (relaciones «business to business», B2B).

> *"El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente sólo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales"* (considerando 50 del RGPD).

La finalidad del tratamiento debe tener una **relación directa entre quienes traten el dato y la entidad** y no entre aquéllos y quien ostente una determinada posición en la empresa. De este modo, el fin del tratamiento debe ser dirigirse a la persona jurídica, siendo el dato de contacto de la persona física únicamente el medio para lograr esa finalidad.

> **Ejemplo:**
> El responsable del tratamiento no está legitimado para utilizar los datos de contacto con el fin de enviar información comercial o publicitaria al "contacto" como persona física, a título individual, sino que el destinatario último ha de ser la persona jurídica.

Cuando, excepcionalmente, la base jurídica del tratamiento sea el **consentimiento**, éste debe ser inequívoco, de modo que requiere una manifestación del afectado o una clara acción afirmativa, pues el RGPD, a diferencia de la normativa anterior, dispone que el silencio, las casillas ya marcadas o la inacción, no deben constituir consentimiento.

> *"La configuración por defecto de los dispositivos y/o la instalación de programas informáticos que facilitan el tratamiento electrónico de datos personales no puede calificarse como consentimiento dado por los trabajadores, ya que el consentimiento requiere una manifestación activa de voluntad. La ausencia de acción (es decir, no cambiar la configuración por defecto) no se puede considerar, en general, como un consentimiento específico para permitir dicho tratamiento"* (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

El consentimiento de las personas trabajadoras, además, debe ser **libre y específico**, no siendo lícita la sustitución del consentimiento individual por un consentimiento indirecto y plural mediante la **negociación colectiva** (STJUE (Gran Sala), de 5 de octubre de 2014, C-397/01 a C-403/01).

El art. 6 del RGPD menciona otras bases jurídicas que podrían excepcionalmente ser invocadas en el marco de la relación laboral, como la protección de **intereses vitales** del afectado o de otra persona física.

3. LA INFORMACIÓN SOBRE EL TRATAMIENTO DE DATOS PERSONALES

El responsable del tratamiento, normalmente el empleador, debe **informar** a las personas trabajadoras, de forma **concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo**, sobre el tratamiento de datos que está llevando a cabo (arts. 13 y 14 del RGPD[2]).

> *"La información facilitada a un interesado no debe contener lenguaje o terminología de naturaleza excesivamente legal, técnica o especializada, y deben evitarse expresiones indefinidas como «podría», «algunos», «frecuentemente» y «posible»"* (Directrices sobre la transparencia en virtud del Reglamento 2016/679 del Grupo de Trabajo del Artículo 29[3]).

El deber de información forma parte del **contenido esencial** del derecho a la protección de datos y constituye una **garantía** para el afectado, ya que le permite conocer qué datos están siendo tratados sobre su persona, con quién los comparte el empleador y, además, los derechos de los afectados y cómo ejercerlos.

Es recomendable adoptar un modelo de **información por capas**, mediante una primera capa con información básica, facilitada en el mismo momento en el que se recojan los datos, y una segunda capa más detallada.

En cuanto a los plazos:

1. Cuando los datos se **obtengan del afectado** (por ejemplo, a través del currículum vitae) la información debe proporcionarse en el **mismo momento** en que el empleador recabe los datos.

2. Cuando los datos **no se obtengan del afectado** la información debe proporcionarse dentro de un **plazo razonable**, y a más tardar en el plazo de **un mes**, con las siguientes precisiones:

a) Si los datos personales han de utilizarse para una comunicación con el afectado, debe informarse a más tardar en el momento de la primera comunicación a dicho afectado.

b) Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

En principio, la inclusión de cláusulas informativas de protección de datos en el **contrato** de trabajo, o en un anexo al mismo, es un **medio adecuado para cumplir con el derecho de información** de las personas trabajadoras.

[1] Véanse en el RGPD
[2] Ratificadas por el Comité Europeo de Protección de Datos

No obstante, cuando, excepcionalmente, un determinado tratamiento de datos exceda de lo necesario para el cumplimiento del contrato de trabajo es necesario contar con una base jurídica para efectuar dicho tratamiento, como puede ser el consentimiento. Se debe tener en cuenta que la **información no equivale al consentimiento**, por lo que la incorporación en el contrato de trabajo de la información relativa a este tipo de tratamientos no es por sí misma una base jurídica.

Por ello, lo apropiado es separar el contrato de trabajo de otros documentos a través de los cuales el empleador solicite a la persona trabajadora el consentimiento para poder realizar tratamientos no comprendidos dentro de la ejecución de la concreta relación laboral de que se trate en cada caso.

Ejemplo.
Una empresa formaliza un convenio gracias al cual la persona trabajadora obtiene ventajas para ciertas compras, pero requiere confirmación de la identidad del beneficiario. Ese tratamiento de datos no es necesario para el cumplimiento del contrato de trabajo, y por ello se necesita el consentimiento de la persona trabajadora. Dicho consentimiento no puede exigirse dentro del contrato de trabajo, como una cláusula más, para garantizar que la manifestación de voluntad de la persona trabajadora sea libre, inequívoca y específica.

La empresa debe informar sobre los **nuevos tratamientos** de datos personales que decida realizar con carácter posterior al nacimiento de la relación laboral (véase **4.1**).

Más información en la Guía para el cumplimiento del deber de informar.

4. DERECHOS DE PROTECCIÓN DE DATOS EN EL ÁMBITO LABORAL

Las personas trabajadoras pueden ejercer los siguientes derechos ante el responsable del tratamiento:

Derecho de acceso
(art. 15 RGPD)

Con independencia de la información proporcionada, la persona trabajadora tiene derecho a la confirmación de que se está produciendo un tratamiento de datos y, en caso de que así sea, derecho a conocer cómo se está produciendo ese tratamiento con un contenido similar al del derecho de información.

Las personas trabajadoras que ejerciten el derecho de acceso pueden solicitar una **copia de los datos** personales que están siendo objeto de tratamiento.

Los responsables podrán atender a este derecho facilitando el acceso remoto a un sistema seguro que ofrezca al afectado un acceso directo a sus datos personales.

Derecho de rectificación
(art. 16 RGPD)

Las personas trabajadoras pueden exigir la rectificación de los datos inexactos que estén siendo objeto de tratamiento, así como que se completen aquellos que sean incompletos.

Derecho de supresión
(art. 17 RGPD)

Las personas trabajadoras pueden exigir la **supresión** de los datos personales objeto de tratamiento en las situaciones siguientes:

- Cuando los datos personales ya **no sean necesarios** en relación con los fines para los que fueron recogidos o tratados de otro modo.

- Cuando la base jurídica para el tratamiento de datos sea el **consentimiento** y la persona trabajadora lo haya retirado.

- Cuando el tratamiento de datos sea **ilícito**.

- En el caso de que la persona trabajadora se **oponga al tratamiento de datos** que no sean necesarios para el cumplimiento y ejecución del contrato de trabajo.

- Cuando los datos personales debieran ser **suprimidos** en cumplimiento de una obligación legal.

Por exigencia legal, cuando se proceda a la rectificación o supresión de los datos personales, éstos deben **bloquearse**. En concreto, el bloqueo de los datos consiste en la «identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas» (art. 32 de la LOPDGDD). Transcurrido ese, plazo es el momento de proceder a la destrucción de los datos.

De este modo, el procedimiento de supresión debe contemplar el período de bloqueo, lo que implica:

a) Una exigencia de concreción sobre el periodo de uso de los datos y el momento en el que cesa la finalidad que legitimó su tratamiento.

Ejemplo.
El final de la relación laboral conlleva la desaparición de la base jurídica que justificaba el tratamiento de datos.

b) Una previsión sobre el **período de conservación** de los datos, una vez que desaparece la base jurídica que legitimaba el tratamiento previo, si alguna obligación legal exige dicha conservación. En virtud del art. 17.3.b) del RGPD, en estos supuestos no procederá atender el derecho de supresión.

Ejemplo.
El art. 21 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, tipifica como infracción leve "no conservar, durante cuatro años, la documentación o los registros o soportes informáticos en que se hayan transmitido los correspondientes datos que acrediten el cumplimiento de las obligaciones en materia de afiliación, altas, bajas o variaciones que, en su caso, se produjeran en relación con dichas materias, así como los documentos de cotización y los recibos justificativos del pago de salarios y del pago delegado de prestaciones". Durante ese plazo no procede la supresión de los datos.

c) El **período de bloqueo**, cuya duración está en directa relación con la **prescripción de las acciones** para la exigencia de responsabilidades derivadas del tratamiento.

Ejemplo.
Las obligaciones tributarias prescriben a los 4 años. Por tanto, los datos relativos a las retenciones practicadas a las personas trabajadoras deberían bloquearse por un periodo de 4 años a partir de la fecha límite para presentar la declaración de cada ejercicio. Cuando este plazo no exista, o cuando sea inferior a un año, se tendrán en cuenta los plazos de prescripción de las infracciones a la LOPDGDD, que en el caso de las muy graves es de tres años (art. 78 LOPDGDD), sin perjuicio de que pudieran derivarse otras obligaciones o responsabilidades, por ejemplo, en el marco de procedimientos administrativos o judiciales.

d) Los datos no pueden **manipularse ni alterarse** durante el período de bloqueo. En ese período no se admite el tratamiento de datos, sino únicamente su puesta a disposición de las autoridades competentes, cuando proceda.

Derecho a la limitación del tratamiento

(art. 18 RGPD)

La limitación del tratamiento consiste en "*el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro*" (art. 4.3 del RGPD) Es un derecho de las personas trabajadoras que se puede ejercer frente al empleador, en las situaciones siguientes:

- **Inexactitud** de los datos personales puesta de manifiesto por la persona trabajadora, produciéndose la limitación del tratamiento durante un plazo que permita al responsable la pertinente verificación.

- **Ilicitud** del tratamiento por parte del empleador con petición de la persona trabajadora de limitación de uso y no de supresión de los datos.

- **Cuando los datos personales ya no son necesarios para los fines del tratamiento**, pero existe interés de la persona trabajadora en su conservación para la formulación, el ejercicio o la defensa de reclamaciones.

- **Oposición** al tratamiento de datos por parte de la persona trabajadora mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del afectado.

Las personas trabajadoras tienen derecho a ser **informadas** acerca de cualquier rectificación o supresión de datos personales o limitación del tratamiento, así como del levantamiento de la limitación.

Derecho a la portabilidad de los datos

(art. 20 RGPD)

Cuando la base jurídica del tratamiento sea el consentimiento o la ejecución de un contrato, la persona trabajadora tiene derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a **transmitirlos a otro responsable del tratamiento** sin que lo impida el responsable al que se los hubiera facilitado, siempre que el tratamiento se efectúe por medios automatizados.

Este derecho no exige necesariamente que el responsable comunique los datos a las personas trabajadoras en ese formato, sino que se reconoce al afectado el derecho a que los datos **se transmitan directamente de responsable** a responsable cuando sea técnicamente posible.

Derecho de oposición

(art. 21 RGPD)

Cuando la base jurídica del tratamiento de las personas trabajadoras sea la satisfacción de

intereses legítimos perseguidos por la propia empresa o por un tercero o una misión realizada en interés público, aquellas podrán ejercer el derecho de oposición ante la empresa que estará obligada a dejar de tratar los datos, salvo que acredite motivos legítimos que prevalezcan sobre los intereses, los derechos y las libertades de las personas trabajadoras o para la formulación, el ejercicio o la defensa de reclamaciones.

Derecho a no ser objeto de decisiones individuales automatizadas

(art. 22 RGPD)

Este derecho pretende garantizar que el afectado no sea objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de forma similar.

Constituye una elaboración de perfiles cualquier forma de tratamiento de los datos personales que evalúe aspectos personales, como, en particular, analizar o predecir aspectos relacionados con el rendimiento en el trabajo.

Hay que tener en cuenta que este derecho no será aplicable cuando la decisión automatizada sea necesaria para la celebración o ejecución de un contrato o se base en el consentimiento explícito del afectado (aunque en estos casos el responsable debe garantizar el derecho del afectado a obtener intervención humana, expresar su punto de vista e impugnar la decisión), o esté autorizado por ley.

Más información sobre el ejercicio de derechos en "Conoce tus derechos".

5. EL PRINCIPIO DE MINIMIZACIÓN Y SU IMPACTO EN LA RELACIÓN LABORAL

La ejecución del contrato de trabajo es la base jurídica principal para el tratamiento de datos personales en la relación laboral. Sin embargo, ello no implica que el empleador pueda conocer cualquier tipo de dato personal de las personas trabajadoras, porque el **principio de minimización de datos** exige que los datos personales sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (art. 5 del RGPD).

Por tanto, el empleador tiene derecho a conocer los **datos personales necesarios** para el normal desarrollo de la relación laboral, entre ellos, y a título meramente ejemplificativo y no limitativo, los siguientes:

- Nombre y apellidos de la persona trabajadora
- Sexo
- Número de DNI, número de identificación de extranjero y número de afiliación a la Seguridad Social
- Nacionalidad
- Discapacidad
- Fecha de nacimiento

Todos esos datos pueden tener repercusión directa en el cumplimiento de las obligaciones empresariales, por ejemplo, en materia de **actos de encuadramiento afiliación, alta y cotización de la Seguridad Social** para la comprobación de que la persona trabajadora cumple los **requisitos pertinentes para celebrar el contrato entre otros**.

Sin embargo, otros datos personales **no resultan imprescindibles** para la ejecución del contrato de trabajo, como, por ejemplo, el nombre de usuario en las redes sociales o en servicios de mensajería o portales de internet. El tratamiento de estos datos por parte del empleador exige la concurrencia de una **base jurídica** diferente a la ejecución del contrato, como puede ser el interés legítimo, que habrá de demostrarse debidamente atendiendo a los principios de ponderación y proporcionalidad. No obstante, habrá que analizar las **características de cada relación laboral** para determinar qué datos son necesarios para el cumplimiento de ese contrato y cuáles no.

Ejemplo.
El Banco de España puede establecer determinadas cautelas e imponer determinadas obligaciones para comprobar que las personas que trabajan en él respetan las reglas de compatibilidad y sobre acceso y uso de información privilegiada. Sin embargo, esas cautelas y obligaciones han de resultar idóneas, necesarias y proporcionales, requisitos que no cumpliría una exigencia a las personas trabajadoras que implique facilitar datos fiscales o la declaración de IRPF, sin mayores filtros, pues aunque el fin resulte aparentemente legítimo podría dar como resultado que la empresa conozca datos sensibles sin mediar el consentimiento de la persona trabajadora (por ejemplo, aspectos ideológicos o de creencias, como la aportación a la Iglesia Católica o la afiliación sindical). (SAN 4494/2018, de 7 de diciembre, Sala de lo Social).

Son datos personales los que permiten a la empresa **localizar a las personas trabajadoras y contactar con ellas**, como el domicilio, la dirección de correo electrónico, el número de teléfono (fijo y/o móvil) o la cuenta bancaria. En general, parece necesario para la ejecución del contrato que el empleador disponga de alguna vía de comunicación con las personas trabajadoras, y es imprescindible que la persona trabajadora proporcione a la empresa alguna forma de contacto. Sin embargo, el contrato de trabajo no legitima a la empresa para solicitar a la persona trabajadora todos esos datos, como ha puesto de manifiesto el Tribunal Supremo en relación con la **dirección de correo electrónico o el número de teléfono personal** (STS 4086/2015, de 21 de septiembre, Sala de lo Social). Es decir, la necesidad del tratamiento habrá de ponderarse caso a caso.

Para ello, será necesario analizar en cada caso la base jurídica alegada –que podría ser el contrato de trabajo, el consentimiento o el interés legítimo del empleador-, la finalidad pretendida y los datos tratados.

> *"La creación de una base interna de datos de contacto de los empleados de una empresa que contenga el nombre, la dirección laboral, el número de teléfono y la dirección de correo electrónico de todos los empleados, para permitir que los empleados puedan ponerse en contacto con sus compañeros de trabajo, puede en determinadas situaciones considerarse como necesario para la ejecución de un contrato en virtud del artículo 7, letra b), pero también podría ser lícito en virtud del artículo 7, letra f),si se demuestra que prevalece el interés del responsable del tratamiento y se toman todas las medidas adecuadas, incluida, por ejemplo, la consulta a los representantes de los empleados"* (Dictamen 6/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE del Grupo de Trabajo del Artículo 29).

Por otro lado, el tratamiento de datos de familiares o allegados de la persona trabajadora a modo de persona de contacto "para emergencias" (por ejemplo, accidentes) no es estrictamente necesario para la ejecución del contrato, por lo que se requiere el consentimiento de las personas trabajadoras (no el del tercero). Los principios de proporcionalidad y limitación de la finalidad suponen que el trabajador podrá elegir libremente la persona de referencia, sin que deba precisar ante la empresa qué relación le une a ella, y podrá asimismo concretar el modo de contacto (email, teléfono fijo, teléfono móvil), debiendo proporcionar únicamente los datos imprescindibles (por ejemplo, la empresa no necesita conocer el domicilio de esa persona de contacto).

En determinados casos, el empleador puede acreditar un interés legítimo que justifique la necesidad de recoger la dirección de correo electrónico y el número de teléfono particulares de la persona trabajadora, sin que puedan utilizarse posteriormente para fines distintos de aquéllos que motivaron dicha recogida.

En relación con el **número de cuenta bancaria**, se ha venido admitiendo el tratamiento de ese dato personal (Dictamen 6/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE del Grupo de Trabajo del Artículo 29). Sin embargo, los principios de minimización y limitación de la finalidad implican que la empresa únicamente puede proceder a su tratamiento si el salario se abona mediante transferencia, porque debe disponer de los medios a través de los que hacer efectivas las obligaciones correspondientes. En cambio, no podría exigir esa información a las personas trabajadoras cuando el pago se realiza por otra vía que no implique a la entidad bancaria.

Tampoco es lícita la cesión genérica por contrato de los **derechos de imagen**, salvo que esa cesión sea necesaria para la ejecución del contrato.

Ejemplo.
Prestación laboral de carácter comercial que exija videollamadas, habiéndose establecido expresamente en el contrato de trabajo que es con el fin de desarrollar una actividad propia de telemarketing (STS 1436/2019, de 10 de abril, Sala de lo Social).

6. DEBERES Y OBLIGACIONES EN EL ACCESO A DATOS PERSONALES: SECRETO Y SEGURIDAD

El RGPD y la LOPDGDD incluyen el **deber de seguridad** junto con el **deber de secreto** dentro de los **principios de la protección de datos**.

«Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)» (art. 5.1.f) del RGPD).

En particular, el art. 32.1 del RGPD establece que las medidas técnicas y organizativas establecidas han de gestionar el riesgo para los derechos y libertades de las personas físicas, más allá de otras consideraciones de seguridad, como la seguridad para propia organización, el Estado u otros posibles intereses.

En concreto, el art. 5 de la LOPDGDD establece:

1. Los responsables y encargados del tratamiento y todas las personas que intervengan en cualquier fase del tratamiento estarán sujetas al **deber de confidencialidad**.

2. La obligación general de confidencialidad será complementaria de los deberes de **secreto profesional**.

3. Las obligaciones de confidencialidad y de secreto profesional **se mantendrán aun cuando hubiese finalizado la relación** del obligado con el responsable o el encargado del tratamiento.

Ambos deberes resultan necesarios y constituyen una garantía para el derecho fundamental a la protección de datos. El secreto y la confidencialidad aseguran que los datos personales sólo sean conocidos por el afectado y por aquellos usuarios de la organización cuyo perfil les atribuye competencia para usar, consultar, modificar o incluir los datos en los sistemas de información.

Las medidas de seguridad deben garantizar, además de la confidencialidad, la **disponibilidad de los datos**, y con ella su recuperación ante cualquier evento, y su **integridad**, protegiéndolos frente a cualquier manipulación no autorizada. La empresa debe disponer de políticas de cumplimiento de estos dos principios, pues con ellas no sólo se garantiza un derecho fundamental, sino que además se ofrece confianza y seguridad a los afectados. La implementación de medidas de seguridad protege activos que son importantes para la empresa, como los datos de sus clientes y proveedores (STSJ CV 5238/2015 de 11 de noviembre, Sala de los Social).

Para el adecuado cumplimiento de estos dos deberes resulta ineludible disponer de **políticas de gestión de personal** en los que se definan de modo muy claro los perfiles funcionales de cada puesto, y de procedimientos de **formación del personal**.

Las obligaciones de secreto y seguridad en materia de protección de datos constituyen deberes muy específicos vinculados al hecho del propio tratamiento y van más allá del secreto profesional en su concepción tradicional. Su inadecuado cumplimiento pone en riesgo el derecho fundamental a la protección de datos y causa habitualmente un grave perjuicio para la reputación de la empresa.

Ejemplo.
El abandono de documentos sin destruir en la basura común es una de las infracciones más habituales en materia de protección de datos de la que es responsable la empresa.

Por todo ello es muy **recomendable**:

a) **Diseñar las funciones y responsabilidades** de la plantilla de personal en función de su relación con el tratamiento de datos personales.

b) **Formar** adecuadamente a las personas trabajadoras teniendo en cuenta su distinto grado de responsabilidad y garantizando que conozcan sus deberes de seguridad y secreto. La formación debe contribuir a crear una cultura de compromiso con la protección de datos.

c) **Advertir y formar**, incluso a aquellas personas trabajadoras que no teniendo una relación directa con los sistemas de información y los tratamientos de datos personales puedan poner en peligro el secreto o la seguridad de los datos (por ejemplo, el personal de limpieza).

d) Valorar la conveniencia de **designar a un delegado de protección de datos** (por ejemplo, empresa, o grupo empresarial), con un experto formado en la materia que pueda asesorar al en el cumplimiento de la normativa y el principio de responsabilidad proactiva de los responsables del tratamiento

7. TRANSFERENCIAS INTERNACIONALES DE DATOS

Por la incidencia que a lo largo del transcurso de la relación laboral puedan tener, es preciso realizar una mención al régimen de las transferencias internacionales de datos. Tienen tal consideración, las transmisiones de datos personales fuera del Espacio Económico Europeo (EEE), ya constituyan una comunicación de datos a otros responsables del tratamiento, en cuyo caso exportador e importador son responsables del tratamiento, ya tengan por objeto la prestación de servicios por un encargado del tratamiento establecido fuera del EEE. En este último caso el exportador puede ser un responsable o un encargado del tratamiento y el importador de los datos un encargado o subencargado del tratamiento.

El RGPD ha venido a simplificar el régimen de transferencias internacionales, lo que ha supuesto un cambio sustancial en el modelo de control que se llevaba a cabo bajo la normativa anterior. Con el RGPD, se suprime la obligación de notificar a la AEPD las transferencias de datos a países que disponen de una Decisión de adecuación, o si se realizan en aplicación de alguna de las excepciones previstas en el art. 49 del RGPD, salvo cuando, dada su singularidad, las transferencias son realizadas por un responsable del tratamiento por motivos legítimos e imperiosos y siempre que, además, se cumplan el resto de los requisitos que se exigen en el art. 49.1. párrafo segundo del RGPD.

Se suprime también, con carácter general, la obligación de obtener la autorización previa de la AEPD cuando las transferencias se basen en la aportación de garantías adecuadas, que sólo será necesaria cuando las garantías aportadas para la transferencia se recojan en un contrato que no se ajuste al clausulado tipo aprobado por la Comisión Europea, o adoptado por una autoridad de control y aprobado también por la Comisión Europea, o cuando las garantías se incluyan en acuerdos administrativos para transferencias entre autoridades u organismos públicos.

Por tanto, las transferencias internacionales de datos se podrán realizar sin necesidad de autorización de la Autoridad de Control:

- Cuando tengan por destinatario una entidad establecida en alguno de los países o territorios declarados de nivel adecuado de protección por la Comisión Europea.
- Cuando se aporten garantías adecuadas por las que los afectados cuenten con derechos exigibles y acciones legales efectivas mediante:
  - Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos
  - Normas corporativas vinculantes para el caso de compañías multinacionales
  - Cláusulas contractuales tipo adoptadas por la Comisión Europea, o por una autoridad de control y aprobadas por la Comisión Europea
  - Un código de conducta, o un mecanismo de certificación.
- Cuando se diera alguna de las circunstancias excepcionales previstas en el art. 49 del RGPD, como el consentimiento explícito del afectado, o cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del tratamiento.
- Requerirán la autorización previa de la AEPD cuando las garantías adecuadas se aporten mediante:
  - Cláusulas contractuales específicas
  - Acuerdos administrativos entre las autoridades u organismos públicos

De las transferencias internacionales de datos se ha de informar a los afectados e incluirlas en el registro de actividades de tratamiento (arts. 13 y 30 RGPD).

3. SELECCIÓN Y CONTRATACIÓN

1. LÍMITES AL TRATAMIENTO DE DATOS

El primer tratamiento de datos personales se producirá normalmente durante la fase previa a la contratación, esto es, en el **proceso de selección para un puesto de trabajo**.

Para ello deben tenerse en cuenta algunas cautelas:

- El tratamiento de datos personales durante el proceso de selección **no exige el consentimiento** de la persona candidata. La base jurídica es la del art. 6.1.b) del RGPD.

  El tratamiento de datos es lícito cuando resulta necesario para la aplicación a petición de la persona trabajadora de medidas precontractuales o la intención de concluir un contrato (art. 6.1.b RGPD).

  El tratamiento «debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato» (considerando 44 RGPD).

- Es conveniente, cuando los recursos lo permitan, disponer **de impresos tipo** para la formalización del currículo y de un procedimiento para su entrega por las personas candidatas, ya que ello permite no sólo informar adecuadamente, sino también definir con precisión el tipo de datos a tratar, establecer las medidas de seguridad, etc.

- Si para la selección de personal se realiza algún tipo de **anuncio o convocatoria pública**, debería incluirse en ella la información del art. 13 del RGPD.

- Si el currículo se presenta directamente por la persona candidata sin habérsele solicitado, deben fijarse procedimientos de **información** que supongan algún acuse o confirmación de que se han conocido las condiciones en las que se desarrollará el tratamiento.

  Ejemplo.
  Si el currículum se remitió por correo postal o electrónico y se cuenta con una dirección electrónica facilitada por el propio afectado, puede remitírsele información por ese medio, solicitando confirmación de la recepción y condicionando el tratamiento de los datos al acuse de recibo. Si se presentó en un mostrador u oficina de atención, debería ser informado allí por cualquier medio que acredite el cumplimiento de este deber, como por ejemplo carteles o documentos de acuse de recibo.

El **deber de información** deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado (véase **2.3**).

La empresa es responsable de la **custodia** de la documentación entregada por la persona candidata (por ejemplo, el currículum vitae). En caso de pérdida de esa documentación, que contiene datos personales, la empresa incurrirá en **infracción del RGPD (principio de integridad y confidencialidad).**

Únicamente cabe solicitar **datos relevantes** para el desempeño del puesto de trabajo y no información indiscriminada. Deben respetarse los principios de **minimización y limitación de la finalidad**.

Ejemplo.
No es legalmente posible exigir a las personas candidatas a un puesto de trabajo un certificado de antecedentes penales, que no puede ser objeto de tratamiento salvo en aquellos supuestos excepcionales en que, autorizados por una Ley y con las debidas garantías, se contemple dicha medida. En este sentido, existen normativas específicas que lo contemplan, por ejemplo, en lo relativo a seguridad de aeropuertos, en que una norma europea de directa aplicación, como es el Reglamento europeo sobre normas comunes para la seguridad de la aviación civil, impone la medida relativa a la comprobación de los antecedentes personales del personal que accede a zonas restringidas de seguridad. En consecuencia, solamente resultará conforme a lo establecido en la legislación de protección de datos la solicitud de utn certificado de antecedentes penales en el supuesto de que una norma contemple dicha medida. En otro caso, la solicitud vulnera el derecho a la protección de datos. Se admite la solicitud de un certificado de antecedentes penales en determinados trabajos que implican el contacto con menores (art. 13.5 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor) o en la contratación de ciertas personas trabajadoras en entidades que deben asumir obligaciones en la prevención del blanqueo de capitales y de la financiación del terrorismo (art. 40 del Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, aprobado por el Real Decreto 304/2014, de 5 de mayo). La base jurídica para el tratamiento de esos datos desaparece al finalizar la relación laboral.

El tratamiento de datos con **otros fines** exigiría otra base jurídica, como el consentimiento o el interés legítimo.

Ejemplo.
Utilización de los datos de contacto del currículum con fines comerciales o publicitarios.

Se consideran **datos personales las impresiones o valoraciones subjetivas** de quienes llevan a cabo el proceso de selección (STS 7922/2000, de 31 de octubre, Sala de lo Contencioso), por lo que debe garantizarse la transparencia en el tratamiento de esos datos, incluyendo la posibilidad del ejercicio de los derechos de acceso, rectificación, oposición y supresión.

Es habitual que los empleadores soliciten el informe de la vida laboral a las personas candidatas durante el proceso de selección. Debe tenerse en cuenta lo siguiente:

a) La empresa **no está legitimada para obtener ese informe directamente** de la Seguridad Social.

b) El **consentimiento no es una base jurídica válida** en este caso, pues no es completamente libre para la persona trabajadora. La empresa podría acreditar un interés legítimo para solicitar el informe de vida laboral, a los efectos de comprobar la veracidad y la experiencia que la persona candidata refleja en su solicitud.

c) El informe que eventualmente se entregue no necesariamente debe ser completo, sino adaptado al interés legítimo que el empleador demuestre (principio de **minimización de datos**).

Ejemplo.
La empresa podría tener un interés legítimo en comprobar si las personas candidatas cuentan con la experiencia previa que alegan en la concreta actividad que desarrollarían. El informe de

vida laboral podría ser un medio apto para demostrar o comprobar esa experiencia, pero el empleador no necesita conocer todas las ocupaciones de aquéllas, sino sólo las relevantes a esos fines. Además, la exigencia de la vida laboral no se justificaría si las personas candidatas pudieran demostrar esa experiencia por otros medios menos invasivos, como puede ser aportar una carta de recomendación que describa la experiencia que se requiere (principio de proporcionalidad).

2. SELECCIÓN DE PERSONAL Y REDES SOCIALES

Las personas candidatas y las personas trabajadoras no están obligadas a permitir la indagación del empleador en sus perfiles de redes sociales, ni durante el proceso de selección ni durante la ejecución del contrato.

Aunque el perfil en las redes sociales de una persona candidata a un empleo sea de acceso público, el empleador no puede efectuar un tratamiento de los datos obtenidos por esa vía si no cuenta para ello con una **base jurídica válida**. La indagación en los perfiles de redes sociales de las personas candidatas a un empleo sólo se justifica si están relacionados con **fines profesionales**. El tratamiento de los datos obtenidos por esta vía únicamente será posible cuando se demuestre que dicho tratamiento es necesario y pertinente para desempeñar el trabajo. Y la persona trabajadora tiene derecho a ser **informada** sobre ese tratamiento (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

Ejemplo.
Durante la selección de nuevo personal, un empresario comprueba los perfiles de los candidatos en varias redes sociales e incluye información de estas redes (y cualquier otra información disponible en Internet) en el proceso de selección. Sólo si para el puesto de trabajo es necesario revisar la información sobre un candidato en las redes sociales, por ejemplo, para poder evaluar los riesgos específicos de los candidatos respecto de una función específica y los candidatos están correctamente informados (por ejemplo, en el texto del anuncio de trabajo), el empresario puede tener una base jurídica para revisar la información de acceso público relativa a los candidatos» (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

La empresa no está legitimada para solicitar «**amistad**» a personas candidatas para que éstas, por otros medios, proporcionen acceso a los contenidos de sus perfiles (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29). La empresa tampoco está legitimada para solicitar a una persona trabajadora o candidata a un empleo la **información que éste comparta con otras personas a través de las redes sociales**.

3. ENTREVISTAS DE TRABAJO

La persona candidata a un empleo responde a numerosas preguntas durante la entrevista de trabajo, pero esas contestaciones no equivalen a un consentimiento para el tratamiento de sus datos personales. Por tanto, los datos obtenidos por esa vía, directamente o mediante deducciones (por ejemplo, creencias religiosas o afiliación sindical o política), no pueden ser objeto de **tratamiento** si no se dispone de una **base jurídica** (datos necesarios para la ejecución del contrato, interés legítimo o consentimiento).

> "El hecho de someter a una candidata a preguntas familiares y personales totalmente ajenas al trabajo a desempeñar, sea cual sea el lugar de prestación de los servicios (pues ya había manifestado su disponibilidad a desplazarse), supone una conducta discriminatoria, puesto que la trabajadora se ha visto obligada revelar sus planes familiares y datos médicos pertenecientes a su más estricta intimidad, innecesarios para una gestión de personal responsable y respetuosa con la dignidad del empleado" (STSJ ICA 1799/2014, de 7 de abril, Sala de lo Social).

El empleador que solicite datos de carácter personal en los procesos de selección, dando lugar a discriminaciones contrarias al principio constitucional de igualdad, podría incurrir en una infracción administrativa muy grave tipificada en el Texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, aprobado por Real Decreto Legislativo 5/2000, de 4 de agosto (TRLISOS).

Ejemplo.
Constituye infracción administrativa muy grave «solicitar datos de carácter personal en los procesos de selección o establecer condiciones, mediante la publicidad, difusión o por cualquier otro medio, que constituyan discriminaciones para el acceso al empleo por motivos de sexo, origen, incluido el racial o étnico, edad, estado civil, discapacidad, religión o convicciones, opinión política, orientación sexual, afiliación sindical, condición social y lengua dentro del Estado» (art. 16.1.c) TRLISOS).

4. COLABORACIÓN ENTRE EMPRESAS

El proceso de selección y contratación no siempre es realizado directa e íntegramente por el empleador, sino que en ocasiones colaboran otras empresas, como agencias de colocación, empresas dedicadas a la selección de personas trabajadoras, o empresas de trabajo temporal.

En el caso de las **agencias de colocación y empresas de selección**, éstas actuarán como encargadas del tratamiento cuando hayan celebrado previamente un contrato con la empresa que busca personas trabajadoras, que será la que determinará los fines y medios de dicho tratamiento. La agencia de colocación localizará a las personas candidatas interesadas en ese puesto y la base jurídica del tratamiento será el art. 6.1.b) del RGPD, al ser necesario para la celebración del contrato de trabajo, y no el consentimiento. Una vez que desaparece esta base jurídica que legitima el tratamiento de datos, éstos deberán ser **destruidos o devueltos** al responsable del tratamiento, según se haya pactado en el contrato de encargo del tratamiento, debiendo procederse al bloqueo en el primer caso. No obstante, habrán de ser **conservados** cuando exista una previsión legal que así lo exija. También podrán ser conservados si media consentimiento del afectado.

Por el contrario, en aquellos casos en que las agencias de colocación y empresas de selección contacten con las personas candidatas antes de disponer de ofertas de empleo concretas, y por tanto sin un contrato como encargadas del tratamiento previamente celebrado con otra empresa, serán consideradas **responsables del tratamiento** de los datos de la persona candidata.

Asimismo, las **empresas de trabajo temporal (ETT)** serán **responsables del tratamiento**, pues son empleadoras directas de las personas trabajadoras.

Por último, será necesario el **consentimiento** de la persona candidata para que la empresa donde solicita trabajo ceda sus datos (por ejemplo, el currículum a otra, aunque las dos empresas formen parte de un mismo **grupo empresarial**.

Ejemplo.
Así puede suceder en los grupos de empresas cuando la persona candidata a un empleo en una de ellas no obtenga el puesto que había solicitado, pero exista una vacante en otra empresa del grupo.

5. DECISIONES AUTOMATIZADAS

Como se ha señalado anteriormente (véase II.4), el RGPD prohíbe, con carácter general, la toma de decisiones basadas «únicamente en el tratamiento automatizado, incluida la elaboración de perfiles» cuando produzca «efectos jurídicos en el interesado o le afecte significativamente de modo similar» (por ejemplo, ser descartado de un proceso de selección).

No obstante, estas decisiones se podrán llevar a cabo cuando sean necesarias para la celebración o ejecución de un contrato.
En la medida en que se trata de una excepción a la regla general, dicha necesidad debe ser interpretada restrictivamente.

Ejemplo.
Es admisible la decisión automatizada en procesos de selección con numerosos candidatos para realizar una primera criba excluyendo a quienes incumplen alguna condición o requisito esencial, como la ausencia de titulación suficiente (Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 del Grupo de Trabajo del Artículo 29[4]).

No obstante, no resulta admisible que las decisiones basadas en la utilización de **algoritmos** y la elaboración de perfiles en el proceso de selección produzcan **discriminación**. Cuando el resultado de la decisión vulnere derechos fundamentales, el diseño del algoritmo debe ser modificado.

Ejemplo.
Contratación de un número significativamente mayor de hombres que de mujeres.

El procedimiento debe contemplar algún mecanismo de **intervención humana si la persona afectada así lo solicita, además de un cauce para que esta persona exprese su opinión** y, en su caso, **impugne** la decisión. Asimismo, tendrá derecho a recibir una explicación de la decisión tomada después de tal evaluación (considerando 71 del RGPD). Para ser considerada como intervención humana, el responsable del tratamiento debe garantizar que cualquier supervisión de la decisión sea significativa, en vez de ser únicamente un gesto simbólico.
Debe llevarse a cabo por parte de una persona autorizada y competente para modificar la decisión. Como parte del análisis, debe tener en cuenta todos los datos pertinentes.

En el diseño e implementación del algoritmo deberá realizarse una **evaluación de impacto** (art. 35.3 del RGPD).

[4] Ratificadas por el Comité Europeo de Protección de Datos

6. CATEGORÍAS ESPECIALES DE DATOS PERSONALES

Durante el proceso de selección de personal podrían recabarse datos especialmente sensibles.

Principalmente en dos supuestos:

1. Reconocimientos médicos:
Con carácter general, el reconocimiento médico es voluntario para la persona trabajadora, salvo que por ley se establezca como obligatorio (por ejemplo, actividades con riesgo de enfermedad profesional). Sin embargo, el tratamiento de datos no requiere el consentimiento, puesto que el art. 9.2.h) del RGPD admite la recogida y tratamiento de datos con fines de «**medicina preventiva o laboral**» y «**evaluación de la capacidad laboral del trabajador**».

La Recomendación 2015 (2) del Consejo de Europa apto. 9.2) establece que, de conformidad con la legislación nacional, una persona solicitante de empleo sólo puede ser interrogada sobre su estado de salud y/o ser examinado médicamente para:

a. indicar su idoneidad para el empleo futuro;

b. cumplir los requisitos de la medicina preventiva.

2. Pruebas psicotécnicas o psicológicas:
Los test psicotécnicos, de personalidad o las pruebas psicológicas son frecuentes en las entrevistas de trabajo y el tratamiento de datos obtenidos exige el **consentimiento** de la persona afectada. Antes de recabar este tipo de datos es necesario analizar la **proporcionalidad** del tratamiento y la base jurídica para el mismo.

Los datos obtenidos a partir de estas pruebas constituyen datos de salud y, por tanto, especialmente sensibles, por lo que exigen medidas para garantizar la privacidad y la confidencialidad reforzadas.

La persona candidata, además de **ser informada**, tiene derecho a:

- **Acceder a los resultados** de esas pruebas psicotécnicas o psicológicas.
- **Conocer los criterios de selección** utilizados por la empresa.

En cambio, una persona candidata **no tiene derecho a acceder a los resultados de las demás**.

Los **test genéticos** a una persona trabajadora o candidata a un empleo **no son admisibles** por las siguientes razones:

- No concurre una **base jurídica** (el consentimiento no se considera libre).
- No es una **medida proporcional**.
- Permite conocer datos personales irrelevantes o superfluos, no siendo compatibles con el principio de minimización de datos.

7. CONSERVACIÓN DE DATOS EN CASO DE NO CONTRATACIÓN

Una vez c**oncluido el proceso de selección**, si la persona candidata no es contratada, desaparece la base jurídica para el tratamiento de datos, por lo que sería necesario su **consentimiento para un futuro tratamiento** (por ejemplo, incorporación a una bolsa de trabajo), salvo que el empleador pueda demostrar un interés legítimo. En caso contrario, debe **destruir el currículum** y proceder a la **supresión y bloqueo de los datos personales**.

4. DESARROLLO DE LA RELACIÓN LABORAL

1. LA PROTECCIÓN DE DATOS COMO DERECHO DINÁMICO

Las relaciones laborales no son una realidad estática y pueden a estar sujetas a cambios sobrevenidos tanto desde el punto de vista de la persona trabajadora como desde la perspectiva del empleador.

Ejemplo.
Una persona trabajadora que inicialmente no se acogió a la posibilidad de descontar de su nómina la cuota sindical, posteriormente se afilia a un sindicato y solicita dicho descuento.

Ejemplo.
La empresa instala un nuevo sistema de control de presencia basado en el uso de dispositivos de videovigilancia.

Por ello será necesario **informar** a las personas trabajadoras en todos aquellos casos en los que se produzcan cambios que afecten al tratamiento de los datos personales.

Como ya se ha señalado (véase 2.2), el tratamiento de datos personales en la relación laboral no exige el consentimiento de la persona trabajadora si esos datos son necesarios para el cumplimiento y ejecución del contrato.

En todo caso, los datos han de ser **adecuados, pertinentes y limitados** a lo necesario en relación con los fines para los que son tratados.

Ejemplo.
La empresa no necesita en todo caso la dirección de email personal o el número de teléfono privado de la persona trabajadora. Cuando el trabajo le exija disponibilidad personal fuera de su centro u horario de trabajo, una medida más moderada e igual de eficaz para conseguir la comunicación de la empresa con la persona trabajadora sería la puesta a su disposición de un instrumento de trabajo (ej. teléfono de empresa).

No es lícito el tratamiento de **datos superfluos o excesivos**, especialmente cuando por esa vía el empleador pudiera conocer otra información adicional de forma no justificada.

Ejemplo.
Solicitud del empleador a las personas trabajadoras para que aporten datos fiscales o la declaración de IRPF, pues, aunque el fin pudiera resultar legítimo en algunas ocasiones (por ejemplo, comprobar la competencia desleal) podría dar como resultado que el empleador conozca datos sensibles sin mediar el consentimiento de la persona trabajadora (por ejemplo. aspectos ideológicos o de creencias, como la aportación a la Iglesia Católica o la afiliación sindical).

El principio de minimización debe ponerse en relación con el principio de **limitación de la finalidad**, que supone que los datos deben ser recogidos con fines determinados, explícitos y legítimos, y no pueden ser tratados ulteriormente de manera incompatible con dichos fines.

Ejemplo.
El empleador no está legitimado para utilizar los datos de contacto proporcionados por la persona trabajadora con un fin distinto al cumplimiento de las obligaciones o derechos laborales, de modo que vulnera el derecho a la protección de datos que use los datos de contacto para el ofrecimiento de productos o servicios, pues supone dirigirse a la persona trabajadora como cliente o usuaria, y no como persona trabajadora.

El **principio de proporcionalidad** también es un límite al tratamiento de datos o a determinadas órdenes empresariales.

Ejemplo.
No se puede exigir a las personas trabajadoras que utilicen un perfil de redes sociales facilitado por su empresario, incluso cuando pueda justificarse por el contenido de la actividad (por ejemplo, portavoz de una organización). Las personas trabajadoras deben conservar la opción de un perfil «no profesional» y no público que puedan utilizar en lugar del perfil «oficial» relacionado con el empresario, lo que debería especificarse en el contrato de trabajo (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

2. DECISIONES AUTOMATIZADAS RELATIVAS AL RENDIMIENTO LABORAL

Como ya se advirtió (véase III.5), la relación laboral es un ámbito en el que, como excepción, se admiten las **decisiones automatizadas**, y no sólo durante el proceso de contratación, sino también en el transcurso de la relación de trabajo. Esas decisiones automatizadas podrían ser determinantes para las personas trabajadoras que tienen derecho al **ascenso** o sobre la **renovación o extinción** de contratos.

En este proceso se han de incluir las mismas garantías para el afectado que las establecidas en el capítulo 3.5.

3. IDENTIFICACIÓN DE PERSONAS EMPLEADAS ANTE CLIENTES

El empleador podrá exigir que las personas trabajadoras porten **tarjetas identificativas** donde consten su nombre y apellidos, con las siguientes cautelas:

1. Debe tratarse de actividades de **cara al público** o por **razones de seguridad**.

2. La información incluida en la tarjeta deberá ser la **mínima** imprescindible para facilitar la identificación.

Esto puede incluir el tratamiento de **fotografías**, sin necesidad del consentimiento de la persona trabajadora, siempre que se respete el principio de l**imitación de la finalidad**.

4. PUBLICACIÓN DE DATOS DE PRODUCTIVIDAD

En relación con el concepto retributivo de productividad, la publicación de estos datos en relación con las personas trabajadoras debe respetar el derecho a la protección de datos mediante una adecuada ponderación en cada caso concreto, entre el interés legítimo y la lesión de los derechos e intereses de los afectados, como reiteramos a continuación.

Para ello debe tenerse en cuenta lo siguiente (Informe AEPD 183-2018):

1. La **base jurídica** es la satisfacción de intereses legítimos, art. 6.1.f) del RGPD.

2. La apreciación de la «necesidad» del tratamiento exige una **ponderación** entre los intereses del empleador y los intereses y derechos de los afectados, en este caso las personas trabajadoras.

> **Ejemplo.**
> El abono de un complemento de productividad y la publicación de los datos de rendimiento para dotar de transparencia al proceso y motivar a las personas trabajadoras a obtener mejores resultados podría constituir un interés legítimo.

3. La publicidad de los datos de productividad **no puede ser indiscriminada**, sino que debe limitarse a las personas autorizadas.

> **Ejemplo.**
> La publicación debe ajustarse a la finalidad perseguida, por lo que, como regla general, los datos de productividad no pueden publicarse por un medio que permita el acceso de personas distintas a las personas trabajadoras de la empresa.

4. La publicación debe realizarse del modo que resulte **menos perjudicial** para la persona afectada.

> **Ejemplo.**
> Además de evitar la difusión generalizada, la publicación de la productividad no debe contener datos que permitan identificar a la persona trabajadora si el mismo objetivo puede lograrse por medios menos invasivos, por ejemplo, identificando a la persona trabajadoras con un código que sólo conozcan las personas autorizadas (por ejemplo, la propia persona trabajadora, el departamento de recursos humanos, etc.).

5. Debe garantizarse que los datos de productividad **no puedan ser utilizados para futuros tratamientos** con finalidad incompatible de aquella que motivó su recogida.

5. NÓMINAS

En las nóminas no debe figurar información superflua o adicional, diferente a la relación de ingresos y deducciones derivadas del contrato de trabajo. En particular, **no debería incluirse la mención a la afiliación sindical** en el recibo de salarios, siendo recomendable que el eventual descuento de la cuota sindical se identificase de manera que no permitiera a terceros conocer esa información, por cuanto la nómina es exigida habitualmente por entidades públicas y privadas para realizar determinados trámites.

> **Ejemplo.**
> En las nóminas, junto con la información referida a sus retribuciones, podrían aparecer otros datos, como el domicilio fiscal, la cuenta corriente en que se produzca los pagos e incluso datos especialmente protegidos refe-

rentes a salud o ideología, así como el descuento, en su caso, de la cuota sindical de los afiliados a un sindicato. Esos datos no deben ser conocidos por terceros, ni tampoco por determinadas personas cuando la finalidad no lo justifique, si no media consentimiento del afectado. La eventual transparencia sobre las retribuciones y el desglose de los conceptos retributivos, que en determinados ámbitos puede ser incluso una exigencia legal, no se extiende a otros datos personales, aunque figuren en la nómina.

Por otro lado, es muy frecuente que la gestión de las nóminas se encomiende a una **asesoría** o a una **gestoría**. La empresa contratada debe tratar datos personales para poder realizar su prestación, y lo hará en condición de encargada del tratamiento[5].

6. CATEGORÍAS ESPECIALES DE DATOS PERSONALES

El tratamiento de categorías especiales de datos personales (véase 2.1) está prohibido con carácter general. Sin embargo, **es lícito su tratamiento** en las siguientes circunstancias, entre otras (art. 9.2 del RGPD):

1. Con el **consentimiento** del afectado, salvo que una norma expresamente prohíba el tratamiento aun con consentimiento. En este sentido, el art. 9.1 de la LOPDGDD prohíbe el tratamiento de datos, aun con consentimiento del afectado, cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, a fin de evitar situaciones discriminatorias.

Ejemplo.
Aunque no sea una práctica generalizada en las empresas, el consentimiento no podría legitimar en modo alguno el tratamiento de datos que derivase en la creación de una "lista negra" de personas trabajadoras afiliadas a un sindicato, tal y como ya declaró en su día el Tribunal Supremo en relación con la elaboración de listas de personas trabajadoras conflictivas, sindicalizados o que demandan a la empresa en defensa de sus derechos (STS 4686/2015, de 12 de noviembre, Sala de lo Civil)

2. Cuando sea **necesario** para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del **Derecho laboral y de la seguridad y protección social.**

3. Cuando el tratamiento sea necesario para proteger **intereses vitales** del interesado.

4. Cuando sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o **sindical**, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

5. Cuando se refiere a datos personales que el interesado ha hecho **manifiestamente públicos**.

[5] Pueden consultarse las Directrices para la elaboración de contratos entre responsables y encargados del tratamiento

6. Cuando sea necesario para la formulación, el ejercicio o la defensa de **reclamaciones** o cuando los tribunales actúen en ejercicio de su función judicial.

7. Cuando sea necesario para fines de **medicina preventiva o laboral**, **evaluación de la capacidad laboral de la persona trabajadora**, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.

No obstante, el tratamiento de esta clase de datos está sometido a mayores cautelas de las ordinarias y su **publicación** no ha de permitir la identificación del interesado (**datos disociados**).

Por tanto, **ninguna empresa está legitimada para exigir a la persona trabajadora que comunique datos personales** como:

- Afiliación sindical.
- Ideología política.
- Creencias religiosas.
- Orientación sexual.

No obstante, el **ideario** de algunas entidades como, por ejemplo, colegios religiosos, puede incidir en el tratamiento de categorías especiales de datos, ya que es posible que deban tenerse en cuenta a la hora de valorar la procedencia e improcedencia de determinados despidos.

Respecto de los **datos sanitarios**, véase el capítulo 7.

Los datos biométricos

El artículo 4.14 del RGPD recoge la siguiente definición de «**datos biométricos**»:

> «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».

En esta definición, cabe distinguir los supuestos de (i) identificación biométrica y (ii) verificación o autenticación biométrica. La identificación es el proceso de reconocer a un individuo particular entre un grupo, comparándose los datos del individuo a identificar con los datos de cada individuo en el grupo (uno-a-varios). La verificación o autenticación es el proceso de probar que es cierta la identidad reclamada por un individuo, comparándose los datos del individuo únicamente con los datos asociados a la identidad reclamada (uno-a-uno).

Este criterio, que ya se recogía en el Dictamen 3/2012 sobre evolución de tecnologías biométricas del Grupo de Trabajo del Artículo 29, ha sido admitido en el Protocolo de enmienda al convenio para la protección de individuos con respecto al procesamiento de datos personales (Convenio 108+ del Consejo de Europa) y es una diferenciación que se ha incluido en el Libro Blanco sobre inteligencia artificial de la Comisión Europea. Atendiendo a la citada distinción, y de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluye ambos supuestos, tanto la identificación como la verificación/autenticación.

Las Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público, determinan, en su apartado 12, que el concepto de dato biomé-

trico abarca tanto la "autenticación" como la "identificación", y si bien son conceptos distintos, en ambos procedimientos se tratan datos dirigidos a identificar a una persona física, por lo que ambos se incluyen en el concepto de "tratamientos de datos", y más específicamente, son tratamientos de datos personales de categorías especiales.

En caso de que se traten datos biométricos, la AEPD recomienda optar por sistemas de verificación o autenticación biométrica, siendo aconsejable que los sistemas biométricos se basen en la lectura de los datos biométricos almacenados como plantillas cifradas en soportes que puedan ser conservados exclusivamente por las personas trabajadoras (por ejemplo, tarjetas inteligentes o dispositivos similares). Por ejemplo, en el caso del tratamiento de datos biométricos para el fichaje en el momento de acceso al edificio, se utilizarán por la persona trabajadora terminales en los que será necesario tanto la aproximación de la tarjeta como la lectura de la huella. Es decir, el lector generará el identificador numérico de la huella que habrá de corresponderse con el de la tarjeta, entendiéndose que se ha producido el acceso al puesto de trabajo como consecuencia de la coincidencia entre el identificador generado y el que consta en la huella.

En relación con los sistemas de identificación biométrica, como ya se ha señalado, el artículo 9.2.b) del RGPD exceptúa de la prohibición general del tratamiento de datos biométricos de categorías especiales cuando, "el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado".

En este sentido, el art. 20.3 del Real Decreto 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET) establece que «El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad».

Sin embargo, ya estemos ante un sistema de verificación/autenticación o ante uno de identificación, estos tratamientos deben realizarse conforme a las garantías del RGPD y, en particular, las siguientes:

1. El trabajador debe ser informado sobre estos tratamientos en los términos que se han expuesto.

2. Los fabricantes deben implementar la protección de datos «desde el diseño».

> **Ejemplo.**
> Supresión automática de los datos brutos una vez calculada la plantilla, o utilización del cifrado para el almacenamiento de los datos biométricos.

3. Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible. La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares, a fin de garantizar que una persona sólo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.

[6] Más información en el informe AEPD 36/2020

4. El almacenamiento se realizará preferentemente en un dispositivo personal, antes que acudirse a un almacenamiento centralizado. Deberá utilizarse una clave de encriptado específica para los dispositivos de lectura a fin de proteger efectivamente estos datos contra todo acceso no autorizado.

5. El sistema biométrico utilizado y las medidas de seguridad elegidas deberán asegurarse de que no es posible la reutilización de los datos biométricos en cuestión para otra finalidad.

6. Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.

7. Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.

8. Deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

9. Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento y, si fuera posible, deben implementarse mecanismos automatizados de supresión de datos.

Ejemplo.
En el caso de implementación de un sistema biométrico para controlar el acceso a una zona restringida, los datos biométricos de los trabajadores que ya no están autorizados a acceder a esa zona (por ejemplo, por cambio de puesto de trabajo) deben suprimirse (Dictamen 3/2012 sobre evolución de tecnologías biométricas del Grupo de Trabajo del Artículo 29).

10. Si se opta por un sistema de identificación biométrica, será necesario llevar a cabo una evaluación de impacto.

El conjunto de garantías que se han descrito u otras que las complementen puede ser recomendable que se recojan en los convenios colectivos, en este sentido dispone el art. 91 de la LOPDGDD que: «Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral»

7. SISTEMAS INTERNOS DE DENUNCIAS O 'WHISTLEBLOWING'

Estos sistemas se suelen configurar mediante la creación de buzones internos a través de los cuales las personas trabajadoras de la compañía, generalmente mediante un procedimiento online, ponen de manifiesto la comisión, en su seno o en la actuación de terceros que contraten con ella, de actos o conductas contrarios a la ley o al convenio colectivo (art. 24 de la LOPDGDD).

La Ley permite estos sistemas, aunque en todo caso deben respetarse **los principios básicos de la protección de datos**. La base jurídica para el tratamiento de datos es el **interés público** (art. 6.1.e) del RGPD).

Ejemplo.
Con el fin de hacer frente a una sospecha de robo una empresa implementa un sistema de denuncias que ofrece una recompensa a los empleados cuyas denuncias deriven en la identificación de los responsables. Este tipo de sistemas suponen un riesgo para la privacidad de los trabajadores, porque pueden fomentar las acusaciones falsas (Dictamen 6/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE del Grupo de Trabajo del Artículo 29).

La **información** reviste en este caso un carácter primordial. Tanto los denunciantes como los potenciales denunciados deberán haber sido informados previamente de la existencia de estos sistemas y del tratamiento de los datos que conlleva la formulación de una denuncia.

La información puede proporcionarse por varios cauces:

- Directamente en el **contrato de trabajo**.
- **Individual o colectivamente** al implementar o modificar el sistema.
- Mediante **circulares informativas** al personal y a su representación informando de la existencia y finalidad de un tratamiento de datos relacionado con estos buzones o sistemas de denuncias.

Si los datos contenidos en los sistemas de denuncias fueran a ser transmitidos a una tercera compañía que investigue el hecho denunciado se producirá una **comunicación de datos**, de la que el afectado, tanto el denunciante como el denunciado, deberá ser debidamente informado. Esta misma información deberá referirse, en su caso, a la posible transferencia internacional de datos a otras empresas del grupo.

Ejemplo.
Cuando las denuncias sobre vulneración de las normas de protección de datos son transmitidas al "Chief Privacy Officer" que se encuentra en la matriz del grupo.

La existencia de estos buzones debe respetar el **principio de proporcionalidad**, de forma que las denuncias se refieran únicamente a supuestos en que los hechos o actuaciones tengan una efectiva implicación en la relación entre la empresa y el denunciado, concretando así qué acciones deberán ser objeto de denuncia y especificando las normas a las que las denuncias podrán referirse, normas que podrían estar recogidas en códigos internos de conducta.

Ejemplo.
En sistemas concernientes al personal, sería necesario que los buzones de denuncias se refiriesen a actuaciones que pudieran conducir a una sanción a la persona trabajadora, o inclusive a la resolución de su contrato.

Ha de respetarse el **principio de limitación de la finalidad**, por lo que no cabe utilizar la información obtenida por esta vía con fines distintos a los que motivaron la implementación del sistema.

La **LOPDGDD admite sistemas de denuncias anónimas**. En caso de que la denuncia no sea anónima, la **confidencialidad de la información del denunciante** debe quedar a salvo, no facilitándose su identificación al denunciado.

Precisamente, como consecuencia de lo anterior, será necesario adoptar medidas que proporcionen la adecuada **seguridad y confidencialidad** de la información, pudiendo implementarse medidas reforzadas de seguridad y extremando las cautelas que garanticen el cumplimiento del deber de secreto.

El acceso a los datos debe limitarse exclusivamente a quienes desarrollen las funciones de control interno y de cumplimiento, o al encargado del tratamiento, que eventualmente se designen a tal efecto.

Únicamente será lícito el acceso de otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.

Ejemplo.

Pueden adoptarse medidas como:

- limitar el acceso al contenido de las denuncias a los usuarios que lleven a cabo la investigación y relacionarlos en el documento de seguridad;
- establecer un sistema de registro de accesos;
- firma de compromisos reforzados de confidencialidad con los usuarios autorizados, con especiales medidas disuasorias para el caso de vulnerarse el deber de secreto.

El personal con funciones de **gestión y control de recursos humanos** sólo podrá acceder a dichos datos en caso de procedimientos disciplinarios contra una persona trabajadora, sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo.

La **conservación** del dato debe limitarse al tiempo necesario para la investigación de los hechos y, sólo en caso de que de aquélla se desprenda la adopción de determinadas medidas contra el denunciado, sería posible conservar los datos por un plazo superior, debiendo eliminarse en caso contrario. En todo caso, los datos **deben suprimirse transcurridos tres meses** desde su introducción en el sistema de denuncias sin que se aplique la obligación de bloqueo, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada.

Ejemplo.

En caso de que la investigación de una denuncia contra un directivo pueda dar lugar a un procedimiento de despido o a la exigencia de responsabilidades civiles sí será posible tratar los datos una vez acreditada en la investigación la realidad de los hechos denunciados en tanto persista la posibilidad de interponer acciones civiles o laborales. No obstante, los datos no pueden conservarse en el propio sistema de información de denuncias internas.

Deberán garantizarse los **derechos de acceso, rectificación, supresión y oposición** del denunciado, sin que ello implique revelar la identidad del denunciante. En todo caso, el denunciado debería poder conocer en el menor tiempo posible el hecho que se le imputa a fin de poder defender debidamente sus intereses.

Aclaración.

Debe facilitarse al denunciado esta información tras un tiempo prudencial en que se lleve a cabo la investigación preliminar de los hechos.

8. REGISTRO DE JORNADA

El registro de jornada con el que deben contar todas las empresas de conformidad con lo dispuesto en el art. 34.9 del ET, en su redacción dada por el Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, tiene su base jurídica en una obligación legal de incluir el **horario concreto de inicio y finalización de la jornada** de cada persona trabajadora. Los registros de ese tiempo de trabajo deben ser **conservados** durante cuatro años y permanecer a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social, siendo válido cualquier medio de conservación siempre que se garantice su preservación y la fiabilidad e invariabilidad a posteriori de su contenido, ya se trate de soporte físico o cualquier otro que asegure idénticas garantías.

La Inspección de Trabajo y Seguridad Social ha dictado, con fecha 10 de junio de 2019, el Criterio técnico 101/2019 sobre la actuación de la Inspección de Trabajo y de la Seguridad Social, en materia de registro de jornada.

Esos registros suponen un **tratamiento de datos**, porque permiten identificar a una persona en concreto.

Desde la perspectiva del derecho a la protección de datos debe tenerse en cuenta:

1. El derecho a la protección de datos no limita las opciones de una empresa en relación con el sistema de registro horario, aunque es recomendable que se adopte el sistema **menos invasivo** posible.

2. La **base jurídica** es la citada obligación legal y no el consentimiento de las personas trabajadoras.

3. Las reglas de protección de datos no pueden impedir la transmisión de la información pertinente a la **Inspección de Trabajo y Seguridad Social**, cuando así lo reclame en el ejercicio de sus funciones (art. 18 de la Ley 23/2015, de 21 de julio, ordenadora del sistema de Inspección de Trabajo y Seguridad Social) (STJUE de 30 de mayo de 2013, C 342/12).

4. La persona trabajadora tendrá derecho a ser **informada** y, en su caso, a ejercitar los derechos de acceso, rectificación, oposición y supresión, con independencia de que el registro sea más o menos sofisticado.

5. El registro de jornada debe estar incluido en el **Registro de las Actividades del Tratamiento** (art. 30 RGPD).

6. En atención al número de trabajadores y al concreto formato empleado (por ejemplo, datos biométricos) podría ser necesario realizar una evaluación de impacto (art. 35.3 RGPD).

7. El registro de jornada no debe incluir más datos personales que los imprescindibles (principio de **minimización**).

8. El registro **no puede ser de acceso público ni estar situado en un lugar visible** para cualesquiera personas trabajadoras, clientes o proveedores.

9. La empresa empleadora actuará como **responsable del tratamiento** respecto de las personas trabajadoras, sin perjuicio de que los proveedores externos de los sistemas de registro se conviertan en encargados del tratamiento con las obligaciones que respectivamente incumben a unos y otros.

10. Los datos del registro no pueden ser utilizados con **finalidades distintas** al control de la jornada de trabajo (principio de **limitación de la finalidad**). El registro horario es un instrumento para verificar la jornada laboral diaria realizada por cada persona trabajadora y su finalidad, como se señala en la Guía elaborada por el entonces Ministerio de Trabajo, Migraciones y Seguridad Social sobre registro de jornada, es crear un marco de seguridad jurídica en las

recíprocas relaciones de personas trabajadoras y empresas, así como posibilitar el control por parte de la Inspección de Trabajo y Seguridad Social. Además, la empresa, tras analizar los datos de registro de jornada, podrá conocer si alguna de las personas trabajadoras ha incumplido su horario y, por este motivo, no es necesario que la persona trabajadora haya sido informada específicamente sobre los resultados de dicho control. Sin embargo, el registro horario no podría ser utilizado para fines diferentes, como por ejemplo comprobar la ubicación de una persona trabajadora.

Ejemplo.
Una persona trabajadora itinerante cuyo registro de jornada se realiza por geolocalización. La finalidad del registro de jornada es comprobar cuándo la persona trabajadora comienza y finaliza el tiempo de trabajo, pero no verificar dónde se encuentra en cada momento. Es un instrumento de comprobación del tiempo de trabajo y no del lugar donde se desarrolla la actividad.

En el marco del artículo 34.9 del E.T., el acceso al registro de jornada por parte de los representantes de las personas trabajadoras incluirá los datos personales necesarios para que puedan cumplir su labor de comprobar la adecuación de los registros a la legalidad vigente en materia de jornada, remuneración, cotización y horas extraordinarias.

Así, tal y como establece la guía del Ministerio de Trabajo sobre registro de jornada:

> «La exigencia de que permanezcan a disposición debe interpretarse en el sentido de que sea posible acceder a los mismos en cualquier momento en que se soliciten por los trabajadores, sus representantes o la Inspección de Trabajo y Seguridad Social, garantizando el empresario su cumplimiento, que será coherente con el sistema de registro utilizado. Esta obligación está establecida directa y expresamente en la Ley por lo que no puede ser condicionada en ningún caso. En este sentido, que los registros "permanecerán a disposición" debe interpretarse en el sentido de estar y permanecer físicamente en el centro de trabajo, o ser accesibles desde el mismo de forma inmediata. Con ello, se evita, además, la posibilidad de la creación posterior, manipulación o alteración de los registros».

11. Las **medidas de seguridad** en los tratamientos con la finalidad del control de jornada dependen del sistema utilizado y del concreto tipo de datos objeto de tratamiento. Deberá evitarse el acceso de personas no autorizadas, inclusive las propias personas trabajadoras si ese acceso permite comprobar datos de otros compañeros.

12. La empresa debe respetar la **confidencialidad** de los datos del registro. La publicidad de esos datos está limitada a las personas autorizadas por ley (personas trabajadoras interesadas, sus representantes y las entidades o autoridades públicas que necesiten tales datos a efectos de una investigación, como la Inspección del Trabajo y Seguridad Social o los jueces).

13. El **delegado de protección de datos** debería estar presente en todo el ciclo de vida de la documentación vinculada con el registro horario, desde el asesoramiento a la dirección de la empresa para la confección y custodia de esta documentación, la resolución de incidencias que se puedan plantear internamente, hasta la función de interlocución con la AEPD.

Cada empresa, previo análisis de sus circunstancias (número de personas trabajadoras, funciones o trabajo que se desarrolla, nivel de seguridad requerido en las instalaciones, medios disponibles para el control laboral, etc.), mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empleador previa consulta con los represen-

tantes legales de las personas trabajadoras en la empresa, se organizará y documentará este registro de jornada.

> **Ejemplo.**
> Es posible un registro horario "a distancia" para personas trabajadoras que no acudan físicamente al puesto de trabajo (por ejemplo, teletrabajo, comerciales, etc.) a través de acceso remoto a una intranet corporativa, o de aplicaciones en dispositivos digitales que deberán garantizar adecuadamente el derecho a la intimidad y a la protección de datos de las personas trabajadoras, de acuerdo con los principios de idoneidad, necesidad y proporcionalidad de los medios utilizados.

En función de cuál sea la configuración concreta del registro horario, la empresa deberá cumplir con **exigencias diferentes** en materia de protección de datos.

9. REGISTRO DE SALARIOS

El art. 28.2 del ET y el Real Decreto 902/2020, de 13 de octubre, de igualdad retributiva entre mujeres y hombres, obligan al empleador a llevar un **registro de salarios**. En relación con la protección de datos personales conviene tener en cuenta:

1. Es una **obligación legal**, por lo que el empleador no requiere el consentimiento de las personas trabajadoras.

2. El registro de salarios **no justifica el tratamiento de datos personales** y la norma que lo regula no es una base jurídica para ello, pues en dicho registro no ha de constar el salario de cada persona trabajadora, sino los «**valores medios**» de los salarios, los complementos salariales y las percepciones extrasalariales de la plantilla «desagregados por sexo y distribuidos por grupos profesionales, categorías profesionales o puestos de trabajo iguales o de igual valor».

3. Es un registro donde deben figurar **datos disociados** y no datos personales, ni información que permita identificar a una persona.

4. No se contempla un derecho a la información, ni el ejercicio de derechos de acceso, rectificación, oposición y supresión, pues no se produce un tratamiento de datos personales.

5. En cuanto a la consulta del registro salarial, el art. 5.3 del Real Decreto 902/2020, señala que en las empresas que cuenten con representación legal de las personas trabajadoras el acceso al registro se facilitará a éstas a través de la citada representación, teniendo derecho a conocer el contenido íntegro del mismo. Y, cuando se solicite el acceso al registro por parte de la persona trabajadora por inexistencia de representación legal, la información que se facilite por parte de la empresa no será de los datos promediados respecto a las cuantías efectivas de las retribuciones que constan en el registro, sino que la información a facilitar se limitará a las diferencias porcentuales que existieran en las retribuciones promediadas de hombres y mujeres, que también deberán estar desagregadas en atención a la naturaleza de la retribución y el sistema de clasificación aplicable.

> **El registro de salario regulado en el art. 28.2 ET no tiene porqué implicar el tratamiento de datos, no obstante, el dato disociado podría convertirse en dato personal respecto de aquellas categorías o grupos profesionales con un reducido número de personas trabajadoras.**

Por ejemplo, una o incluso dos de distinto sexo), pues serían en tal caso perfectamente identificables por mera deducción para todo el que pudiera acceder al registro.

Cuando ello sucediera:

- El registro debería contar con las **medidas de seguridad** basadas en el análisis de riesgos conforme al RGPD.
- El empleador debería **informar** a las personas trabajadoras del tratamiento de datos personales y de su finalidad.
- Los representantes de las personas trabajadoras estarían obligados a respetar la **confidencialidad** acerca de esa información.

10. CONCESIÓN DE AYUDAS DE ACCIÓN SOCIAL

La solicitud de la persona trabajadora de ayudas de acción social implica un tratamiento de datos vinculado a las cargas familiares y a las rentas, cuya **base jurídica** no es el consentimiento, sino el propio **contrato de trabajo** y el **cumplimiento de las obligaciones legales o las previsiones de los Convenios Colectivos** correspondientes.

La persona trabajadora tiene derecho a ser **informada** sobre todos los aspectos relevantes en materia de protección de datos, como la identidad del responsable del tratamiento, su base jurídica, la finalidad, el tiempo de conservación de los datos o los derechos de acceso, rectificación, oposición o supresión.

Los **representantes de las personas trabajadoras** tienen derecho, según dispone el art. 64.7.b) del ET a participar en la gestión o tramitación de la ayuda social de la empresa y, por ello, a acceder a un listado de las personas trabajadoras beneficiarias de la acción social en el ejercicio de las funciones representativas, lo que sucederá cuando el convenio colectivo les concediera un papel en la gestión o tramitación de la ayuda social de la empresa.

No obstante, el principio de minimización de datos aconseja no proceder a una información masiva o indiscriminada, sino que, tal y como señala la STS 111/2018 de 7 febrero, Sala de los Social,

sólo procederá la comunicación de aquellos datos personales que sean necesarios para desarrollar el cometido que tienen atribuido y en la medida en que resulte imprescindible para el ejercicio de sus funciones.

En otros casos será suficiente la cesión de información debidamente disociada que permita a los representantes conocer las circunstancias cuya vigilancia le ha sido encomendada (véase capítulo 6).

En relación con la publicidad en la concesión de estas ayudas, deben distinguirse dos escenarios:

1. En aquellos procesos que **no sean de concurrencia competitiva** y, por tanto, sin un número máximo de solicitudes a aceptar por parte la empresa, la notificación deberá ser individualizada, de modo que los datos personales no deben ser accesibles por terceros.

2. En procesos de **concurrencia competitiva**, es decir, cuando la empresa limite el número máximo de ayudas en atención al cumplimiento de determinados requisitos, los solicitantes –y nunca los terceros al procedimiento- podrán conocer el listado de adjudicación de las ayudas, pero no datos superfluos o no imprescindibles (por ejemplo, el número de DNI).

Por consiguiente, las empresas **no pueden publicar** el listado de ayudas adjudicadas y denegadas en una **página web de libre acceso**, o en un tablón de anuncios situado en una **zona abierta al público**, porque ello permitiría que terceros ajenos al procedimiento pudieran acceder a datos personales.

En el caso de que las ayudas se vinculen con **categorías especiales de datos** (por ejemplo, ayudas por hijos discapacitados) la publicidad de la concesión de la ayuda no ha de permitir la identificación del afectado (datos disociados), por lo que no se podrá publicar ningún dato que permita esa identificación (nombre, número del DNI, pasaporte, etc.).

11. DERECHOS DE CONCILIACIÓN Y CORRESPONSABILIDAD

El tratamiento de datos personales de la persona trabajadora por parte de la empresa es necesario para la concesión y gestión de solicitudes relativas a la suspensión del contrato (**suspensión y excedencias**, arts. 45 a 47 del ET), **permisos** (art.37 del ET) y **modificaciones de jornada** (art. 34.8 del ET), que tienen como finalidad la articulación de derechos de conciliación de la vida laboral, personal y familiar.

En muchos supuestos, el ejercicio de estos derechos implica el tratamiento de datos personales de un tercero, como hecho causante de los mismos.

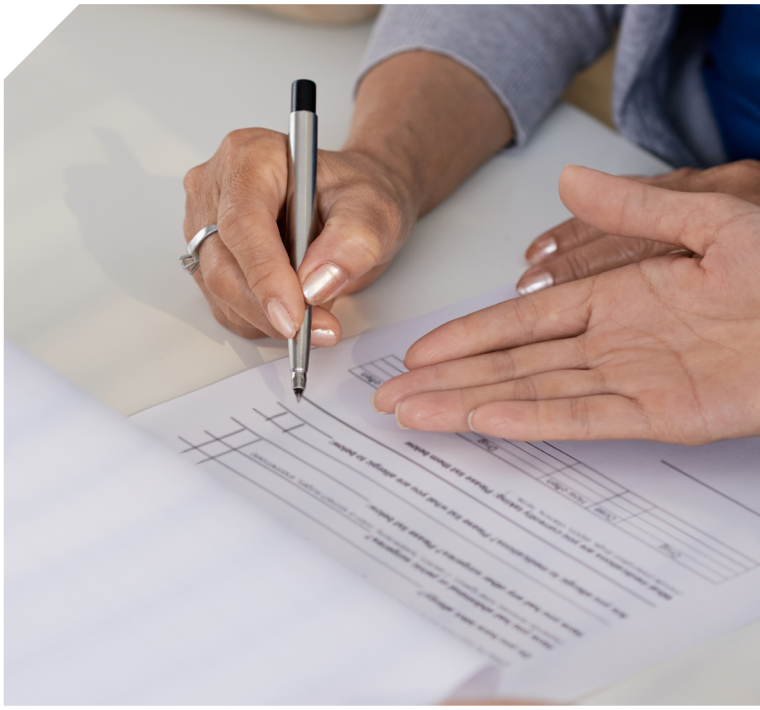
El **tratamiento de estos datos** es imprescindible para el cumplimiento de las obligaciones de la empresa en cuanto a la concesión y gestión del ejercicio de estos derechos de conciliación y corresponsabilidad de las personas trabajadoras.

En cuanto a la cesión de **datos de terceros ajenos a la relación laboral** y que son **sujetos causantes del ejercicio de los derechos de conciliación y corresponsabilidad por la persona trabajadora**, la exigencia legal de acompañar en la solicitud que realice el trabajador aquellos elementos suficientes para que la empresa pueda ponderar la idoneidad de su disfrute implica que ésta tenga acceso a los datos personales que justifican dichos derechos. Así ocurre, por ejemplo, en la acreditación de la necesidad de adaptar la jornada laboral a las necesidades de los hijos o hijas menores de 12 años y las de la vida familiar del artículo 34.8 del ET, o en las excedencias del artículo 46.3 del ET para el cuidado de familiares que sufran un accidente, enfermedad o discapacidad. Por tanto, puede implicar el tratamiento de categorías especiales de datos.

La base jurídica de dichos tratamientos vendrá legitimada por resultar un tratamiento necesario para la ejecución de un contrato en el que la persona trabajadora es parte en relación con el cumplimiento de una obligación legal aplicable al responsable del tratamiento (arts. 6.1.b) y c) del RGPD).

En cuanto al tratamiento de categorías especiales de datos, la circunstancia que exceptúa la prohibición general de su tratamiento es la prevista en el artículo 9.2.b) del RGPD. Los convenios colectivos podrán establecer garantías específicas para el respeto de los derechos fundamentales y de los intereses de los afectados.

En aplicación del **principio de minimización de datos**, se deben recabar los datos estrictamente necesarios para ponderar y justificar el ejercicio del derecho.



12. CONTRATACIÓN DE SEGUROS DE VIDA Y PENSIONES

Es relativamente frecuente la existencia de planes de seguros de vida y planes de pensiones organizados por las empresas en beneficio de las personas empleadas, bien de modo voluntario, bien en virtud de lo pactado en un convenio colectivo.

Debe tenerse en cuenta que:

1. La **base jurídica** del tratamiento de datos depende de la circunstancia que motive la contratación de ese seguro y será, o bien el pacto entre empleador y la persona trabajadora por el que aquél se comprometa a esa contratación, o bien la obligación que derive de un convenio colectivo, en cuyo caso, el consentimiento no es necesario para este tratamiento de datos.

2. La empresa puede realizar distintos **tipos de tratamientos**:

a) La **comunicación de los datos** de identificación y contacto de la persona trabajadora a la empresa aseguradora o la gestora del plan de pensiones.

> **Ejemplo.**
> La empresa se limita a facilitar, previa información a las personas trabajadoras, los datos de estos a la aseguradora o gestora para que, a su vez, ésta inicie su relación con el asegurado o partícipe del plan y recabe los datos que resulten necesarios.

b) La **recogida de datos** vinculados al contrato a celebrar para su traslado a la aseguradora o gestora del plan de pensiones.

> **Ejemplo.**
> Poniendo a disposición de la persona trabajadora la ficha o solicitud de adhesión al seguro de vida colectivo que deberá cumplimentar con cuantos datos resulten necesarios, por ejemplo, los relativos a los beneficiarios.

3. Es necesario en todo caso **informar** a las personas trabajadoras en la recogida de datos, teniendo en cuenta la existencia de distintas posibilidades:

a) En el **contrato de trabajo**. Debe recordarse que cuando se requiera el consentimiento, por no fundamentarse el tratamiento en los deberes u obligaciones de las partes en una relación laboral, el contrato no es el instrumento más idóneo. De utilizarse, deberá informarse expresamente de los términos en los que debe ejercerse el derecho de oposición.

b) Mediante la elaboración de **información específica** dirigida a personas trabajadoras.

4. Pueden existir tratamientos que afecten a **familiares o personas relacionadas con las personas trabajadoras** cuando éstas deban designar beneficiarios del seguro o del plan de pensiones. En este caso el tratamiento de sus datos resulta legitimado por la existencia de la relación laboral, si bien debe recordarse que los datos deben ser estrictamente los necesarios (**minimización**) y únicamente en relación con la contratación del seguro o plan de pensiones (**limitación de la finalidad**).

> **Ejemplo.**
> La AEPD ha considerado que la referencia a las "partes" de una relación jurídica puede considerarse equivalente a los "elementos personales" de dicha relación, de modo que, cuando la relación es formalizada por un afectado en beneficio de un tercero, el tratamiento de los datos de éste, que resulta

necesario para la adecuada formalización de la relación, podría considerarse amparado por la legislación de protección de datos. Por tanto, el tratamiento de los datos del beneficiario de un seguro de vida no requeriría que el beneficiario haya prestado su consentimiento al tratamiento (Informe AEPD 363/2008).

Otra finalidad legítima para el tratamiento de datos personales de miembros de la familia de las personas trabajadoras puede ser la de evitar potenciales conflictos de intereses, si bien debe garantizarse la proporcionalidad, debe respetarse el derecho de información, los datos no pueden utilizarse con finalidad distinta, ni tampoco exceder del ámbito de la empresa.

5. Debe definirse con **precisión el procedimiento para la captación y tratamiento** de los datos personales, optando por el método más eficaz para garantizar los derechos de los afectados.

Desde el punto de vista de un tratamiento absolutamente respetuoso con el derecho fundamental, la opción óptima consiste en ceder a la aseguradora, o a la gestora del plan de pensiones, únicamente los datos de los asegurados o partícipes del plan de pensiones, dejando en sus manos el desarrollo de ulteriores gestiones e informando previamente a las personas trabajadoras.

13. CESIÓN DE DATOS A OTRAS EMPRESAS (GRUPOS DE EMPRESAS, CONTRATAS Y TRANSMISIÓN DE EMPRESAS)

Grupos de empresas

El RGPD menciona expresamente a los grupos de empresas en varios pasajes, admitiendo incluso la designación de un único **delegado de protección de datos** para todas las empresas del grupo (art. 37.2).

El RGPD alude a los grupos de empresas en relación con la consulta previa a la autoridad de control (art. 36), con el contenido de las normas corporativas vinculantes (art. 47), con la designación del delegado de protección de datos (art. 37) y con la comunicación de datos entre las empresas del grupo (art. 88).

El grupo de empresas no constituye una persona jurídica, sino que **cada empresa** del grupo tiene personalidad jurídica propia y puede ser considerada como **responsable del tratamiento** de los datos de las personas trabajadoras siempre y cuando decida sobre los fines y medios del tratamiento (Informe AEPD 494-2008). Por su parte, será considerada como encargado del tratamiento la empresa del grupo que realice el tratamiento (que puede consistir en el almacenamiento y gestión de los datos personales) por cuenta o encargo de otra u otras.

Con carácter general, la comunicación de los datos entre empresas del mismo grupo exigirá acreditar un interés legítimo bien del responsable del tratamiento, o bien del tercero al que se comunican los datos. Ese interés legítimo puede consistir en la centralización de las actividades de carácter administrativo.

Ejemplo.
«Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados» (considerando 48 del RGPD).

Ahora bien, no es acorde al derecho a la protección de datos una organización interna de un grupo empresarial que **centralice la información** de todas las personas trabajadoras en un solo fichero, de modo que quien acceda al mismo pueda comprobar datos de las personas trabajadoras de las distintas empresas sin los filtros pertinentes, salvo que se celebre un contrato como encargado del tratamiento del tratamiento.

A continuación, se recogen unos criterios generales sobre las bases jurídicas para el tratamiento de datos en los grupos empresariales. si bien su aplicación exige analizar y tener en cuenta las circunstancias de cada caso concreto.

La base jurídica dentro de los grupos de empresas podría ser el **cumplimiento del contrato de trabajo**, en caso de que el grupo o varias de sus empresas ocupen la posición de empleador único en la relación laboral, dependiendo del caso concreto. Habrá que tomar en consideración factores como la estructura del grupo de empresas (horizontal o jerarquizado), la finalidad del tratamiento de datos o la movilidad de la persona trabajadora por distintas empresas del grupo.

En el caso de grupos jerarquizados, y en particular cuando la **empresa matriz** tome decisiones directamente, puede ser necesario que disponga de la información pertinente, y entre ella de datos como el tipo de contrato, el salario, la jornada, la productividad, la antigüedad y otros de carácter profesional que puedan ser relevantes para la toma de decisiones.

La base jurídica sería el propio contrato de trabajo en caso de grupos que ocultan una realidad empresarial única, pero únicamente cabe el tratamiento de los datos imprescindibles para el concreto proceso de toma de decisiones (minimización). La persona trabajadora debe ser **informada**.

Cuando se produce una **prestación de servicios indiferenciada** en varias empresas del grupo, la comunicación de datos entre esas empresas resulta lícita, porque es necesaria para el cumplimiento y ejecución del contrato de trabajo. Pero la comunicación de esos datos debe respetar el **principio de minimización** y no pueden ser utilizados con una **finalidad incompatible**.

Se considera como buena práctica la creación de procedimientos internos dentro del grupo para que el ejercicio de los derechos de acceso, rectificación, oposición y supresión por parte de la persona trabajadora en una empresa tenga efectos generales en todo el grupo. En esta línea, el art. del 88 RGPD encomienda a los convenios colectivos la tarea de incorporar normas relativas a la **transparencia del tratamiento** y a la **transferencia de los datos personales dentro de un grupo empresarial** o de una unión de empresas dedicadas a una actividad económica conjunta.

En todo caso, los criterios antes señalados no serán aplicables cuando se constate que la actividad de las empresas, bajo una mera apariencia formal, encubre supuestos ilícitos de empresas aparentes con ánimo de fraude, o cesiones ilegales, que conlleven la no realización efectiva de los tratamientos que se han descrito.

Transmisión de empresas

La comunicación de datos no requiere consentimiento de los afectados en supuestos de **subrogación empresarial**:

1. La **base jurídica** no es el consentimiento de la persona trabajadora, sino la obligación establecida en el art. 44 del ET, el convenio colectivo o el pliego de cláusulas, según los casos.

2. El nuevo empleador tiene derecho a conocer y tratar datos personales de las personas trabajadoras **imprescindibles** para la ejecución y mantenimiento del contrato.

3. La cesión de datos no es lícita si la persona trabajadora rechaza la subrogación y decide permanecer en la empresa cedente.

4. Las personas trabajadoras y sus representantes legales deben ser **informados** de la cesión de datos.

Subcontratación

El art. 42 del ET establece diversas obligaciones y responsabilidades en supuestos de **contratas y subcontratas relativas a la «propia actividad»** de la empresa principal.

El cumplimiento de esas obligaciones legales (art. 6.1.c) del RGPD), puede exigir la comunicación de datos personales de las personas trabajadoras entre el empleador principal y otras empresas de la cadena de contratas, pues la responsabilidad solidaria alcanza a la empresa principal.

Deben distinguirse dos supuestos:

- El momento previo a la contratación o subcontratación (art. 42.1 del ET).
- En momentos posteriores respecto de la responsabilidad solidaria de las obligaciones de naturaleza salarial y las contraídas con la Seguridad Social (art. 42.2 del ET).

En relación con la responsabilidad solidaria de las obligaciones de naturaleza salarial y de las contraídas con la Seguridad Social, existiría una legitimación para la comunicación de datos de las personas trabajadoras entre las distintas empresas que forman la cadena de contratación que deriva del cumplimiento de una obligación legal prevista en el artículo 42 del ET. Este precepto impone a la empresa principal una **responsabilidad solidaria** por las deudas salariales y de Seguridad Social contraídas por las empresas contratistas y subcontratistas durante la vigencia de la contrata. Por su parte, el art. 168 del texto refundido de la Ley General de la Seguridad Social, aprobado por Real Decreto Legislativo 8/2015, de 30 de octubre (TRLGSS), impone una **responsabilidad subsidiaria** en materia de prestaciones de Seguridad Social. Para hacer frente a esas responsabilidades es necesario conocer esas deudas y, por tanto, la comunicación de los datos correspondientes no requiere el consentimiento de la persona trabajadora.

De esta manera, a la obligación de comprobar. previamente a la contratación, que las empresas subcontratadas se encuentran al corriente en el pago de cuotas a la Seguridad Social de las personas empleadas en la contrata por parte del empleador principal, se añade la posibilidad de comprobar que el subcontratista ha cursado su afiliación y alta en la Seguridad Social.

Esta legitimación alcanzaría a los documentos de cotización y nóminas de las personas trabajadoras que pueden contener datos de salud y también datos relativos a la afiliación sindical del personal, siendo este último necesario para que el empleador deduzca en la nómina la cuota sindical de la persona trabajadora.

La legitimación para su tratamiento, al tratarse de categorías especiales de datos personales, sería el art. 9.2.b) en relación con el art. 6.1.c) del RGPD, de manera que el tratamiento de los datos de categorías especiales resulta necesario para el cumplimiento de una obligación legal y el ejercicio de los derechos del responsable en el ámbito del Derecho laboral y de la seguridad y protección social.

El contratista principal tiene la obligación legal de responder solidariamente junto con la empresa subcontratada de las obligaciones salariales y de la Seguridad Social, en los términos previstos en el artículo 42 del ET, mientras dure el periodo de vigencia de la contrata, por ello, la cesión de los documentos de cotización y nóminas está amparada en esta obligación legal impuesta en el ET y el propio TRLGSS.

En todo caso, la comunicación de datos debe respetar el **principio de minimización**, por lo que el acceso por parte del contratista debería limitarse a los datos relacionados con las personas trabajadoras subcontratadas y no a cualesquiera personas trabajadoras de la empresa subcontratada.

14. ACCESO A DATOS DE OTRAS PERSONAS CANDIDATAS A UN PUESTO DE TRABAJO (ACCESO AL EMPLEO O PROMOCIÓN PROFESIONAL)

La sentencia del Tribunal de Justicia de la Unión Europea, de **19 de abril de 2012, C-415/2010**, interpretando las Directivas 2000/43, 2000/78 y 2006/54, reconoció a las personas trabajadoras el derecho a conocer la información pertinente para fundar una reclamación cuando consideren que han sido discriminados en el acceso al empleo o en la promoción profesional.

Por tanto, en esos procesos de **concurrencia competitiva** el perjudicado tendría derecho a conocer, si así lo reclama, información sobre la cualificación profesional de las otras personas candidatas y, en particular, de quienes han obtenido mayor valoración.

Este derecho debe ser compatible con la protección de datos, de modo que:

1. El acceso a esa información **no requiere el consentimiento** de los afectados, pues la **base jurídica** del tratamiento es la «satisfacción de **intereses legítimos** perseguidos por el responsable del tratamiento o por un **tercero**» (art. 6.1.f RGPD).

2. Sólo debe permitirse el acceso a los **datos** relevantes para la tutela de los derechos e intereses que se entienden vulnerados (**principio de minimización de datos**).

3. No se podrán utilizar los datos para una **finalidad distinta** a la de la defensa del derecho.

4. En la medida de lo posible, deben proporcionarse **datos disociados**.

Por tanto, **no debe proporcionarse al solicitante un currículum completo de las otras personas candidatas**, sino limitado a la formación, experiencia profesional y los datos estrictamente relevantes para formalizar la reclamación. No deberá permitirse el acceso como regla general a la siguiente información:

- Nombre
- Fotografía
- Dirección postal o de correo electrónico

En cambio, dependiendo de cuál sea la **finalidad de la reclamación** (discriminación por razón de sexo, de raza, de edad, etc.), persona trabajadora puede acceder a datos personales como la edad, el país de nacimiento, la raza o el sexo de la persona candidata elegida, pero no necesariamente a todos esos datos simultáneamente, sino solamente a los verdaderamente relevantes.

En general, el empleador n**o puede difundir datos personales de una persona trabajadora entre sus compañeros sin consentimiento del afectado**.

15. PROTECCIÓN DE LA PRIVACIDAD DE LAS VÍCTIMAS DE ACOSO EN EL TRABAJO Y DE LAS MUJERES SUPERVIVIENTES A LA VIOLENCIA DE GÉNERO

Los datos personales relativos a las víctimas de acoso en el trabajo y a las mujeres supervivientes a la violencia de género, y en particular su identidad, tienen, con carácter general, la consideración de **categorías especiales de datos personales** y, en todo caso, son datos sensibles que exigen una protección reforzada (Informe AEPD 149 - 2019).

En supuestos de **acoso en el ámbito laboral**, en sus distintas modalidades, el empleador habrá de adoptar las medidas oportunas respecto del acosador, pero también de la persona acosada. Entre esas medidas se encuentra la obligación de **proteger los datos personales**.

El tratamiento de datos personales en supuestos de acoso debe tener en cuenta lo siguiente:

1. La puesta en marcha de **procedimientos sancionadores** en la empresa frente al acosador **no requiere del consentimiento** de la persona acosada. La base jurídica es el cumplimiento de una obligación legal (art. 6.1.c) del RGPD).

La obligación de la empresa está ligada a su posición de garante de salud y seguridad en el trabajo, conforme a los artículos 4.2.d) del ET y 14 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (LPRL) (las personas trabajadoras tienen derecho a una protección eficaz en materia de seguridad y salud en el trabajo).

La empresa está obligada a prevenir e identificar las prácticas de acoso y a erradicar, en su caso, las situaciones de acoso en la empresa. La Sentencia STC 74/2007, de 16 de abril de 2007, apreció la responsabilidad empresarial por omisión.

En este sentido, las organizaciones tienen el deber de colaborar con las autoridades competentes para la erradicación de estas situaciones: la AEPD, las FCSE, las autoridades judiciales. Asimismo, tienen el deber de denunciar cuando sean conocedores de situaciones de ciberacoso en casos de violencia de género.

Además, las entidades tienen el deber de poner en marcha los mecanismos de actuación previstos en sus políticas de prevención del acoso, iniciando las actuaciones disciplinarias pertinentes contra las personas trabajadoras que llevaren a cabo estas conductas y comunicán-

doles las posibles consecuencias jurídicas y responsabilidades en que pudieran incurrir.

2. En la investigación sobre lo sucedido sólo se podrá solicitar a la persona acosada **información pertinente** para el esclarecimiento de los hechos.

3. Los datos de la víctima obtenidos durante la investigación no se podrán utilizar para una **finalidad distinta** a la del procedimiento sancionador, sin perjuicio de las restantes obligaciones legales que incumben a la empresa (como la obligación de poner los hechos en conocimiento de la Justicia en caso de tratarse de un delito público).

Si la conducta fuera constitutiva de delito público, toda persona que la presenciare está obligada a ponerlo en conocimiento de la Justicia. Asimismo, cuando otros delitos, incluidos los leves, se cometan en el ámbito de la violencia de género y doméstica deberán ponerse igualmente en conocimiento de la Justicia.

4. La empresa debe garantizar la **confidencialidad**. La **identidad de la víctima** sólo será revelada ante las personas con interés en el procedimiento, no siendo admisible una publicidad masiva o indiscriminada sin consentimiento de la víctima, ni tampoco el acceso a los datos de personas no legitimadas.

5. Deberá asignarse un **código identificativo** tanto a la persona supuestamente acosada como a la supuestamente acosadora, con objeto de preservar la identidad de estas.

6. La víctima debe prestar su consentimiento para **declarar o testificar** en los procedimientos sancionadores frente al acosador.

7. Una vez concluido el procedimiento sancionador, los datos deben ser **bloqueados** durante el período de prescripción de la sanción, o en tanto puedan ser utilizados en un procedimiento judicial.

8. La **identidad de la víctima** de acoso no deberá constar en ningún documento que se utilice con finalidad distinta a la sanción a la persona acosadora.

9. Como garantía del principio de confidencialidad, tampoco debería figurar el acoso como razón para la adopción de medidas correctoras en el puesto de trabajo.

10. Los **representantes de las personas trabajadoras** únicamente podrán conocer la identidad de la víctima de acoso si es imprescindible para el ejercicio de sus labores de representación.

11. La empresa debe **informar** a la persona acosada y a la supuestamente acosadora sobre el tratamiento de datos y sobre el ejercicio de los derechos de acceso, rectificación, oposición y supresión. No obstante, el derecho de supresión no puede ser ejercitado si la empresa decide sancionar al acosador, pues en tal caso la base jurídica del tratamiento no es el consentimiento, sino el cumplimiento de una obligación legal y la ejecución del contrato de trabajo, en el que se incluye el ejercicio de la potestad sancionadora.

12. Cuando la persona acosada ha recibido asistencia sanitaria derivada de esa situación por parte de los servicios médicos de la empresa, los **datos médicos** constituyen datos personales de categoría especial que sólo pueden ser objeto de tratamiento con una finalidad vinculada al acoso.

Ejemplo.
Prueba en el proceso sancionador frente al acosador.

13. La **cesión de los datos** de la víctima requiere su consentimiento, salvo previsión legal en contra.

Ejemplo.
Solicitud de datos por parte de un juez en el procedimiento penal frente al acosador.

Es recomendable la elaboración de **protocolos** frente a situaciones de acoso donde consten específicamente las medidas a adoptar para la protección de datos personales.

Más información en el Canal Prioritario para comunicar la difusión de contenido sensible en internet y solicitar su retirada y en las Recomendaciones de protección de datos en las políticas de prevención del acoso digital.

En un sentido análogo, el empleador podrá conocer y tratar los datos de una trabajadora vinculados a la condición de **mujer superviviente a la violencia de género** cuando así resulte necesario para el cumplimiento de las obligaciones legales pertinentes; modificación del tiempo de trabajo, traslado, reordenación del tiempo de trabajo, suspensión o extinción del contrato, bonificaciones por contratos de interinidad para sustituir a las trabajadoras supervivientes a la violencia de género. En tales casos:

1. El tratamiento de datos personales sólo procede cuando la trabajadora solicita **ejercitar un derecho** reconocido por esa condición de superviviente a la violencia de género, o cuando el empleador tiene un **interés legítimo y siempre que dicha condición se haya comunicado voluntariamente por parte de la trabajadora**.

Ejemplo.
Comunicación a la entidad gestora a efectos de aplicar reducciones en las cuotas de cotización a la Seguridad Social.

2. El empleador no podrá exigir más datos que la **acreditación de la condición** de mujer superviviente a la violencia de género.

3. La empresa no podrá tratar esos datos con una **finalidad distinta** de la establecida en las leyes.

4. La condición de superviviente a la de violencia de género **no será revelada** por el empleador sin consentimiento de la trabajadora si no es exigencia para el cumplimiento de las obligaciones correspondientes.

5. La documentación de la empresa debe evitar la expresión "superviviente a la violencia de género" y sustituirla por un **código o referencia** que no permita que terceros puedan asociar con la superviviente esa condición.

6. Una vez concluida la relación laboral debe procederse al **bloqueo/supresión** de los datos.

7. Los **representantes** de las personas trabajadoras únicamente podrán conocer la identidad de la superviviente a la violencia de género cuando sea imprescindible para el ejercicio de sus labores de representación.

8. La empresa debe **informar** a la superviviente a la violencia de género sobre el tratamiento de datos y sobre el ejercicio de los derechos de acceso, rectificación, oposición y supresión.

9. A diferencia de las situaciones de acoso, la superviviente a la violencia de género puede ejercitar el **derecho de supresión** en cualquier momento.

Los datos personales de las mujeres supervivientes de violencia de género deben ser objeto de tratamiento con mucha cautela, pues cabría incluso incurrir en delito por un tratamiento inadecuado.

Más información en la Guía "Protección de datos y prevención de delitos".

16. EXTINCIÓN DE LA RELACIÓN LABORAL

El derecho a la protección de datos incide también en el momento de extinción de la relación laboral, pues debe tenerse en cuenta lo siguiente:

1. La **carta de despido** puede contener **datos personales** de la persona despedida y de terceros (por ejemplo, clientes) siempre que sean **adecuados y pertinentes** para esa finalidad, y no datos personales superfluos o irrelevantes. La ley exige que la carta de despido contenga los «hechos que lo motivan».

Ejemplo.
Evidentemente, no podrán constar en la carta de despido datos personales que el empleador no está legitimado para conocer, máxime cuando se trate de categorías especiales de datos personales, como el diagnóstico médico concreto que motiva un despido por ineptitud (STS 5138/2005, de 22 de julio, Sala de lo Social).

2. Deben implementarse las **medidas de seguridad** necesarias para que la carta de despido no sea accesible por terceros no legitimados.

Ejemplo.
El empleador incurre en infracción administrativa si envía la carta de despido a un destinatario equivocado.

3. A la finalización de la relación laboral debe procederse al **bloqueo de los datos** (art. 32 de la LOPDGDD). No obstante, el tratamiento de datos tras la extinción del contrato podría ser admisible si existe otra base jurídica, como sucederá si el empleador demuestra un **interés legítimo**.

Ejemplo.
Un empresario sigue los perfiles de LinkedIn de sus personas extrabajadoras con cláusulas de no competencia durante el período de vigencia de estas con el fin de controlar el cumplimiento de dichas cláusulas. El control se limita a estas personas. Se admite esta fórmula siempre que el empresario pueda demostrar que dicho control es necesario para proteger sus intereses legítimos, que no existen otros medios menos invasivos y que las personas extrabajadoras han sido adecuadamente informadas del alcance del control periódico de sus comunicaciones públicas (Dictamen 2/2017 del Grupo de Trabajo del Artículo 29).

Asimismo, el empleador podrá recabar el **consentimiento** de la persona trabajadora para contactar con ella en el futuro. El empleador debe informarlas de esa circunstancia, que podrían optar por no prestar su consentimiento. La comunicación de datos de un antiguo empleador a un futuro empleador requiere el consentimiento del trabajador.

17. CESIÓN DE DATOS DE PERSONAS EXEMPLEADAS A EMPRESAS DE RECOLOCACIÓN

Las empresas que lleven a cabo un despido colectivo que afecte a más de 50 personas trabajadoras deben ofrecer a los afectados un **plan de recolocación externa** a través de empresas autorizadas. Estos planes de recolocación deben garantizar a las personas despedidas un servicio continuado durante un periodo mínimo de seis meses que incluya medidas de formación y orientación profesional y ayuda en la búsqueda activa de empleo (art. 51.10 del ET).

La **comunicación de datos** entre la empresa que procede al despido y la empresa de recolocación es un tratamiento de datos que no exige el consentimiento de la persona trabajadora, pues la **base jurídica es el cumplimiento de una obligación legal**.

En todo caso, la persona trabajadora tiene derecho a recibir la **información de la empresa** sobre ese tratamiento de datos y a ejercer los derechos de acceso, rectificación o supresión.

No obstante, ese tratamiento debe respetar el **principio de minimización** de datos, por lo que sólo han de proporcionarse los datos imprescindibles para efectuar el ofrecimiento, como la identidad y una forma de contacto. El tratamiento de otros datos que puedan ser necesarios para desarrollar el plan de recolocación será lícito una vez que la persona trabajadora haya aceptado participar en el mismo.

5. CONTROL DE LA ACTIVIDAD LABORAL

1. CONTROL EMPRESARIAL Y PROTECIÓN DE DATOS

El ET ha atribuido facultades específicas a la empresa que posibilitan el **control** del desarrollo de la prestación laboral. El ejercicio de estas facultades comporta en muchas ocasiones un tratamiento de datos personales.

El consentimiento de la persona trabajadora no es necesario, pues la **base jurídica** para la implantación de medidas de control de las personas trabajadoras y para el tratamiento de los datos personales que en tal contexto sean captados se encuentra en el artículo 20.3 del ET:

> «El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso».

El control empresarial puede ser más o menos sofisticado, pero la implantación de **nuevas tecnologías** incrementa el riesgo de afectación a los derechos de las personas trabajadoras, por su gran potencial invasivo: controles biométricos como la huella dactilar, videovigilancia, geolocalización, etc.

Por ello, la implantación de medidas de control exige realizar un **test de proporcionalidad** en el que debe valorarse si la medida de control:

a) Es susceptible de conseguir el objetivo propuesto (juicio de **idoneidad**).

b) Es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de **necesidad**).

c) Es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de **proporcionalidad** en sentido estricto).

Superado el test, el empleador podrá adoptar la medida de control, pero habrá de respetar el **derecho a la protección de datos** si se produce un tratamiento de datos personales.

En el tratamiento de datos que tiene lugar en supuestos de videovigilancia (art. 89 de la LOPDGDD) y geolocalización (art. 90 de la LOPDGDD), así como en caso de captación de datos biométricos, la AEPD y los tribunales han venido admitiendo distintos supuestos y condiciones para su realización.

A estos efectos, el empleador:

a) Debe **informar** a las personas trabajadoras sobre la finalidad del tratamiento de datos, y por tanto sobre la existencia y propósito de la medida de control.

b) No puede recabar más datos de los **estrictamente necesarios**.

c) No está legitimado para utilizar los datos con **finalidades distintas** del control empresarial.

Estas cautelas se extienden también a cualquier otro medio de control que suponga tratamiento de datos personales.

El art. 88 del RGPD atribuye al convenio colectivo un papel relevante para establecer medidas más protectoras para la persona trabajadora en el tratamiento de datos que se produce al implantar «sistemas de supervisión en el lugar de trabajo».

La **prevención** debería tener mucho más peso que la detección, pues la prevención evita el riesgo de vulneración posterior de derechos fundamentales en la fase de control. Esa prevención se vincula con la **subsidiariedad**, que supone que la medida potencialmente invasiva de derechos fundamentales debe ceder ante medidas preventivas que hagan desaparecer el riesgo.

2. CONTROL DE ACCESO A LAS INSTALACIONES

La empresa **no necesita el consentimiento** de la persona trabajadoras para establecer los controles de acceso que estime convenientes, pero debe respetar los derechos fundamentales.

En este sentido:

a) La **base jurídica** del tratamiento de datos puede ser el **contrato de trabajo**, en relación con el art. 20.3 del ET, cuando la finalidad consiste en el control de las personas trabajadoras, pero también podría ser el **interés legítimo** del empleador, si el propósito fuera distinto, por ejemplo, la protección de los bienes empresariales.

Ejemplo.
Un empresario dispone de una sala de servidores en la que se almacenan en formato digital datos sensibles de la empresa, datos personales de las personas trabajadoras y datos personales de los clientes. Para cumplir las obligaciones legales de proteger los datos contra el acceso no autorizado, el empresario ha instalado un sistema de control de acceso que registra la entrada y salida de las personas trabajadoras que tienen permiso para entrar en la sala. Si desaparecen elementos del equipo o algún dato es objeto de acceso no autorizado, pérdida o robo, los registros guardados por el empresario le permiten determinar quién tuvo acceso a la sala en ese momento. Habida cuenta de que el tratamiento es necesario y no vulnera el derecho a la vida privada de las personas trabajadoras, este puede ser en el interés legítimo si las personas trabajadoras han sido informadas adecuadamente sobre la operación de tratamiento. Sin embargo, la observación continua de la frecuencia y los tiempos exactos de entrada y salida de las personas trabajadoras no puede justificarse si estos datos se utilizan también para otros fines, como la evaluación del desempeño (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

b) Deben evitarse sistemas de acceso **especialmente invasivos** de los derechos fundamentales de las personas trabajadoras si existen otros igualmente eficaces que resulten menos intrusivos.

c) En caso de utilización de **datos biométricos, véase** capítulo 4.6.

3. VIDEOVIGILANCIA

La imagen es un dato personal, ya que identifica o hace identificable a una persona. En este sentido, la instalación de cámaras, con finalidades como la seguridad, el control laboral, el acceso a zonas restringidas captando la matrícula del coche y la imagen del conductor, o incluso la monitorización de una UVI, supondría un tratamiento de datos de carácter personal y, en consecuencia, resultaría de aplicación la normativa de protección de datos.

El tratamiento de datos con fines de videovigilancia se regula en el art. 22 de la LOPDGDD. Según el art. 89 de la LOPDGDD, estas imágenes pueden tratarse para el ejercicio de las funciones de control de las personas trabajadoras, con los siguientes requisitos:

1. La **base jurídica** para el control de las personas trabajadoras mediante videovigilancia es el contrato de trabajo y las facultades legales de control concedidas al empleador (art. 20.3 del ET), por lo que no se requiere el consentimiento.

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

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

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

3. El **principio de minimización** del art. 5 del RGPD requiere que los datos personales tratados sean adecuados, pertinentes y limitados en relación con los fines para los que son tratados.

En el ámbito de la videovigilancia este principio supone:

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

b) Que el responsable analice también los **requisitos técnicos** de las cámaras, ya que el zoom, o las denominadas "cámaras domo" pueden afectar al citado principio de minimización.

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

4. La empresa debe **informar** a las personas trabajadoras y, en su caso, a sus representantes, con carácter previo, y de forma expresa, clara y concisa, acerca de esta medida.

5. En el supuesto de que se haya captado la **comisión flagrante de un acto ilícito** por las personas trabajadoras, se entenderá cumplido el deber de informar cuando se haya colocado un **dispositivo informativo** en lugar suficientemente visible concretando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos.

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

6. Se produce un tratamiento de datos tanto si las cámaras graban imágenes como si las reproducen en **tiempo real**. En cambio, no se aplica la normativa de protección de datos a las **cámaras simuladas**, pues, al no captar imágenes de personas físicas identificadas o identificables,

no tiene lugar un tratamiento de datos personales. En cambio, deberán aplicarse los principios vigentes en materia de protección de datos personales y la normativa sectorial que resulte de aplicación a las cámaras que simplemente estén **desactivadas** y que pueden ser activadas sin esfuerzos excesivos.

7. Está prohibida la instalación de sistemas de grabación de imagen y/o sonido en **lugares destinados al descanso o esparcimiento** de las personas trabajadoras, tales como vestuarios, aseos, comedores y análogos.

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

Cuando se trate de tratamientos de videovigilancia que entrañen un escaso riesgo, como podría ocurrir en comunidades de propietarios o pequeños establecimientos, puede utilizarse la herramienta de la AEPD denominada Facilita RGPD.

9. Si se encarga a un tercero la gestión de las cámaras, ese tercero se convierte en un **encargado del tratamiento**.

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

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

4. GEOLOCALIZACIÓN

El art. 90 de la LOPDGDD permite el uso de sistemas de geolocalización para el **control de las personas trabajadoras**, aunque conviene tener en cuenta lo siguiente:

1. La **base jurídica** del tratamiento de datos no es el consentimiento, sino el contrato de trabajo y las facultades de control de **las personas trabajadoras** atribuidas legalmente a los empleadores.

2. Las **personas trabajadoras** y, en su caso, sus representantes deben ser **informados** de forma expresa, clara e inequívoca acerca de la existencia y características de estos dispositivos.

3. Las **personas trabajadoras** también deberán ser informadas acerca del posible ejercicio de los **derechos de acceso, rectificación, limitación del tratamiento y supresión**.

4. Los **principios de minimización y limitación de la finalidad** son plenamente operativos. Por consiguiente, si la finalidad de la geolocalización es el registro horario, los datos no podrán ser utilizados para verificar la ubicación de la persona trabajadora en cada momento, sino las horas de inicio y fin de la actividad, que es lo que permite la base jurídica del registro horario (art. 34.9 del ET).

5. El **principio de proporcionalidad** exige limitar esta clase de sistemas a aquellas situaciones donde no existan medios menos invasivos.

Ejemplo.
SAN 136/2019 de 6 de febrero, Sala de lo Social, que determina que el sistema de geolocalización implementado por la empresa no supera el juicio de proporcionalidad.

Ejemplo.
El dispositivo de geolocalización podría justificarse en el transporte de mercancías cuando resulte relevante conocer dónde se encuentra el vehículo y en qué momento podrá realizar una determinada entrega. Ello no puede suponer que se facilite un dispositivo de esta naturaleza a todas las personas trabajadoras de la empresa cuando su tipo de prestación no lo haga necesario.

La geolocalización puede no tener como objeto a la persona trabajadora, sino el de ser **herramientas propiedad del empleador,** como vehículos o dispositivos móviles.

> «Los dispositivos de seguimiento de vehículos no son dispositivos para la localización de trabajadores, ya que su función es hacer un seguimiento o vigilar la ubicación de los vehículos en que estén instalados. Los empresarios no deben considerarlos como dispositivos para seguir o el comportamiento o el paradero de los conductores o de otro tipo de personal, por ejemplo, mediante el envío de alertas relacionadas con la velocidad del vehículo» (Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes del Grupo de Trabajo del Artículo 29).

La utilización de esas tecnologías es, en principio, **lícita**.

> «El tratamiento de los datos de localización puede estar justificado si se lleva a cabo formando parte del control del transporte de personas o bienes o de la mejora de la distribución de los recursos para servicios en puntos remotos (por ejemplo, la planificación de operaciones en tiempo real) o cuando se trate de lograr un objetivo de seguridad en relación con el propio empleado o con los bienes o vehículos a su cargo. Por el contrario, el Grupo considera que el tratamiento de datos es excesivo en el caso de que los empleados puedan organizar libremente sus planes de viaje o cuando se lleve a cabo con el único fin de controlar el trabajo de un empleado, siempre que pueda hacerse por otros medios» (Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido del Grupo de Trabajo del Artículo 29).

No obstante, estos medios de control permiten, además, el acceso a otra información, como el comportamiento al volante o incluso una monitorización u observación continua. Por tanto, la **geolocalización aplicada a la herramienta conlleva también la geolocalización y el control del propio trabajador/a**, por lo que han de tenerse en cuenta las siguientes cautelas (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29):

- Debe realizarse una **evaluación de impacto** antes de implementar tecnologías de este tipo cuando para el responsable del tratamiento sea nueva o desconocida. Si el resultado es que la geolocalización resulta necesaria en circunstancias específicas, aún debe evaluarse si el tratamiento de datos resultante cumple los principios de **proporcionalidad** y **subsidiariedad**.

- Los empleadores deben asegurarse de que los datos recogidos a través de esta vía se traten con un **fin específico** y no cuenten con un propósito más amplio que permita la observación continua de las personas trabajadoras.

Ejemplo.
Cuando se permite el uso privado de un vehículo profesional, la medida más importante que puede tomar un empleador para garantizar el cumplimiento de estos principios es ofrecer una exclusión voluntaria: en principio, la persona trabajadora debe tener la posibilidad de desactivar temporalmente el seguimiento de la localización cuando lo justifiquen circunstancias especiales, como la visita a un médico. De esta manera, la persona trabajadora puede proteger por iniciativa propia determinados datos de la localización como privados. El empleador debe asegurarse de que los datos recopilados no se utilicen para un tratamiento posterior ilegítimo, como el seguimiento y la evaluación de las personas trabajadoras.

Es posible que las personas trabajadoras estén autorizadas para utilizar los vehículos de la empresa fuera del horario de trabajo, por ejemplo, para uso personal, dependiendo de las políticas específicas que rijan el uso de dichos vehículos. Cuando exista una base jurídica para controlar la ubicación de los vehículos de las personas trabajadoras fuera de las horas de trabajo (por ejemplo, prevenir robos) el medio de control ha de ser proporcional (por ejemplo, el empleador sólo podría activar la «visibilidad» de la localización accediendo a los datos ya almacenados por el sistema cuando el vehículo salga de una región predefinida y no en todo momento).

Ejemplo.
La STSJ AS 4125/2017, de 27 de diciembre, Sala de lo Social, determina la obligación de la empresa de garantizar que el dispositivo de geolocalización implantado en los vehículos de motor utilizados por los trabajadores no estará operativo a partir del momento en que finalice la jornada laboral. El poder de la empresa para imponer las medidas implantadas de captación y tratamiento de datos finaliza al terminar la jornada laboral, momento en el que también la relación laboral deja de constituir el vínculo entre las partes que ampara al empleador para imponer las medidas implantadas de captación y tratamiento de datos.

- Incluso para los fines especificados, es menester reducir los efectos de las funciones de seguimiento. Los sistemas de seguimiento se pueden diseñar para registrar los datos de localización sin proporcionar al empleador todos los detalles. En tales circunstancias, los datos de localización deben estar disponibles únicamente cuando el dispositivo sea objeto de denuncia o se extravíe.

- Las personas trabajadoras que utilicen herramientas de geolocalización deben ser plenamente informados sobre el seguimiento llevado a cabo y la finalidad de su utilización por parte del empleador.

Ejemplo.
El empleador debe informar claramente a las personas trabajadoras de que se ha instalado un dispositivo de seguimiento en el vehículo de la empresa, y que sus movimientos están siendo registrados mientras lo utilizan (y que, en función de la tecnología utilizada, también puede registrarse su comportamiento al volante). Se aconseja que esta información aparezca en un lugar destacado de cada vehículo, a la vista del conductor.

- No es lícito imponer a la persona trabajadora la obligación de proporcionar medios personales para facilitar la geolocalización (por ejemplo, teléfono móvil),

Ejemplo.
La Sentencia de la Audiencia Nacional, SAN 136/2019, de 6 de febrero, Sala de lo Social, declaró que es contrario al derecho a la protección de datos imponer una cláusula en el contrato que exija a la persona trabajadora comunicar al empresario una dirección de correo electrónico y disponer de un teléfono móvil con conexión a internet para instalar una aplicación de geolocalización que permita a los clientes realizar un seguimiento de los pedidos durante el reparto.

Los **registradores de datos de incidencias** son mecanismos de control que pueden ser especialmente invasivos, pues estos sistemas se instalan en los vehículos y en ocasiones se activan ante acontecimientos concretos, por ejemplo, en respuesta a frenadas repentinas, cambios bruscos de dirección o accidentes, en los que se almacenan los momentos inmediatamente anteriores al incidente, pero también se pueden configurar para controlar de forma continua. Esta información puede utilizarse posteriormente para observar y revisar el comportamiento al volante de una persona trabajadora. Además, muchos de estos sistemas incluyen GPS para hacer un seguimiento de la ubicación instantánea del vehículo y también se pueden almacenar otros detalles correspondientes a la conducción (como la velocidad) para su posterior tratamiento.

Estos dispositivos se han generalizado particularmente en las organizaciones cuyas actividades implican el transporte o tienen flotas importantes de vehículos, pero su licitud requiere la acreditación de un **fin legítimo** y el respeto a los principios de **proporcionalidad** y **minimización**:

Ejemplo.
Una empresa de transporte equipa todos sus vehículos con una cámara de vídeo dentro de la cabina que graba sonido y vídeo. El objetivo del tratamiento de estos datos es mejorar las habilidades de conducción de las personas trabajadoras. Las cámaras están configuradas para conservar grabaciones de los momentos en que se producen incidentes como frenazos repentinos o cambios bruscos de dirección. El interés legítimo de la empresa de controlar a los conductores no prevalece sobre el derecho a la protección de sus datos personales. El control continuo de las personas trabajadoras con estas cámaras no es proporcional, pues existen otros métodos (por ejemplo, la instalación de equipos que impiden el uso de teléfonos móviles) y sistemas de seguridad, como un sistema avanzado de frenado de emergencia o un sistema de advertencia de abandono del carril, que pueden utilizarse para la prevención de accidentes de vehículos, y que pueden ser más adecuados. Además, un vídeo de este tipo tiene una alta probabilidad de dar lugar al tratamiento de datos personales de terceros (como los peatones) y, para tal tratamiento, el interés legítimo de la empresa no es suficiente justificación (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

5. CONTROL DE FALTA DE ASISTENCIA POR ENFERMEDAD O ACCIDENTE

El ET faculta a las empresas para realizar **controles médicos** a las personas trabajadoras que **faltan al trabajo** por enfermedad o accidente.

> «El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por este para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de 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» (art. 20.4 del ET).

Este control **no es equiparable ni sigue las mismas reglas que la vigilancia de la salud en materia de prevención de riesgos laborales**.

Como características de estos controles de absentismo pueden indicarse las siguientes:

- La verificación del estado de enfermedad supone un **tratamiento de datos de salud**, y por tanto de una categoría especial de datos.
- La **base jurídica** para el tratamiento de estos datos es el propio **contrato de trabajo** (art. 6.2.b) del RGPD) en relación con las facultades concedidas por el art. 20.4 del ET, por lo que no se requiere el consentimiento de la persona trabajadora, de manera coherente con la sanción prevista en caso de negativa de la persona trabajadora al reconocimiento.
- La empresa **no está legitimada para conocer los detalles concretos del reconocimiento médico**, sino únicamente la conclusión, esto es, si la persona trabajadora está o no en condiciones psicofísicas de reincorporarse a su puesto de trabajo.
- La incorporación de datos de salud a un fichero con la **única finalidad de realizar controles del absentismo** resulta desproporcionada.

> "*Mediante la creación de la base de datos ahora discutida parece perseguirse un control más eficaz del absentismo laboral, según las facultades que al efecto reconoce al empresario la legislación vigente. En este sentido, lo primero que conviene advertir es que entre dichas facultades no figura la de proceder al almacenamiento en soporte informático de los datos atinentes a la salud de los trabajadores -y en concreto del diagnóstico médico- prescindiendo del consentimiento de éstos. Por otra parte, y con independencia de ello, lo verdaderamente relevante es que la medida adoptada por la empresa, sometida a los cánones establecidos para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, no reviste la consideración de solución idónea, necesaria y proporcionada para la consecución del fin, en este caso, el control del absentismo laboral [SSTC 66/1995, fundamento jurídico 5.; 207/1996, fundamento jurídico 4. E) y 69/1999, fundamento jurídico 4.], pues no se trata de medida de suyo ponderada y equilibrada, ya que de ella no se derivan más beneficios o ventajas para el interés general o para el interés empresarial que perjuicios sobre el invocado derecho a la intimidad*" (**STC 202/1999, de 8 de noviembre**).

> "*(...) A la vista del contenido del fichero, forzoso resulta convenir que su mantenimiento no se dirige a la preservación de la salud de los trabajadores sino al control del absentismo laboral, lo que, por otra parte, resulta plenamente acorde con la denominación "absentismo con baja médica" que recibe el fichero. Consecuentemente, la creación y actualización del fichero, en los términos en que se ha llevado a efecto, no puede ampararse, frente a lo sostenido por la empresa, en la existencia de un interés general (art. 7.3 L.O.R.T.A.D. y, por remisión, arts. 10.11 y 61 L.G.S.), que justificaría la autorización por ley, sin necesidad del consentimiento del trabajador, para el tratamiento*

automatizado de los datos atinentes a su salud, ni tampoco en lo dispuesto en los arts. 22 y 23 de la Ley de Prevención de Riesgos Laborales, habida cuenta de que en el fichero en cuestión no se reflejan los resultados arrojados por la vigilancia periódica -y consentida por los afectados- del estado de salud de los trabajadores en función de los riesgos inherentes a su actividad laboral, sino tan sólo la relación de períodos de suspensión de la relación jurídico-laboral dimanantes de una situación de incapacidad del trabajador". (STSJ M 1928/2019, de 8 de marzo, Sala de lo Social)

El control del absentismo adquiere una relevancia particular cuando se realiza mediante la contratación de un **prestador de servicios externo** ya que, además de cumplir con las obligaciones propias de un encargado del tratamiento, debe atenerse a ciertas condiciones:

1. La **información** a la persona trabajadora debe ser muy precisa e indicar que se trata de un control laboral. La información se referirá a que se están verificando sus condiciones de aptitud por cuenta de la empresa y que el tratamiento de datos se ampara en el art. 20.4 del ET.

2. La incorporación de los datos de salud de la persona trabajadora por parte del prestador de ese servicio a una historia clínica le convierte en responsable del tratamiento.

La **sentencia del Tribunal Supremo STS 481/2018, de 25 de enero, Sala de lo Social**, señala que es totalmente válido que la empresa utilice los servicios médicos de una sociedad externa subcontratada para reconocer a los trabajadores que se ausentan por motivos de salud, siempre que se realice dentro de los límites de la buena fe y sea proporcional con los objetivos buscados.

Por otro lado, las empresas sí están legitimadas para elaborar **estadísticas sobre el índice de absentismo** y sus causas.

El comité de empresa tiene derecho a ser informado "de las estadísticas sobre el índice de absentismo y las causas, los accidentes de trabajo y enfermedades profesionales y sus consecuencias, los índices de siniestralidad, los estudios periódicos o especiales del medio ambiente laboral y los mecanismos de prevención que se utilicen" (art. 64 ET). Por su parte, los delegados de prevención tienen derecho a acceder "a la información y documentación relativa a las condiciones de trabajo que sean necesarias para el ejercicio de sus funciones" (art. 36 de la LPRL).

Esas **estadísticas** no han de contener datos personales, sino **datos disociados** que no permitan la identificación concreta de las personas trabajadoras.

6. DETECTIVES PRIVADOS

El art. 20.3 del ET habilita al empleador para adoptar medidas de control y vigilancia de muy distinta intensidad, y entre ellas podría recurrir a un **detective privado**, con las siguientes cautelas:

1. Esta medida, como cualquier otra de control, exige la superación del **test de proporcionalidad**, por lo que no se justifica si existen otras igualmente idóneas, pero menos invasivas.

2. El tratamiento de datos **no requiere el consentimiento** de las personas trabajadoras, pues la base jurídica es el contrato de trabajo, en relación con el art. 20.3 del ET.

3. Está **prohibido investigar** «la **vida íntima** de las personas que transcurra en sus domicilios u otros lugares reservados», así como utilizar «en este tipo de servicios medios personales, materiales o técnicos de tal forma que atenten contra el 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» (art. 49.4 de la Ley 5/2014, de 4 de abril, de seguridad privada).

En relación con el **informe del detective privado** (art. 49 de la Ley 5/2014, de 4 de abril):

- Únicamente se hará constar **información directamente relacionada con el objeto y finalidad de la investigación** contratada, sin incluir en él referencias, informaciones o datos que hayan podido averiguarse relativos al cliente o al sujeto investigado, en particular los de carácter personal especialmente protegidos, que no resulten necesarios o que no guarden directa relación con dicho objeto y finalidad ni con el interés legítimo alegado para la contratación.

- Deberán **conservarse, al menos, durante tres años**, las imágenes y los sonidos grabados durante las investigaciones, salvo que estén relacionadas con un procedimiento judicial, una investigación policial o un procedimiento sancionador. Todo ello sin perjuicio de las reglas sobre bloqueo de datos.

- Las investigaciones privadas tendrán **carácter reservado** y los datos obtenidos sólo se podrán poner a disposición del cliente o, en su caso, de los órganos judiciales y policiales, en este último supuesto únicamente para una investigación policial o para un procedimiento sancionador.

En todo caso, su actividad deberá adecuarse a las obligaciones previstas en el RGPD y en la LOPDGDD, así como a las previsiones y garantías de la de la Ley 5/2014, de 4 de abril.

6. REPRESENTACIÓN UNITARIA Y SINDICAL DE LAS PERSONAS TRABAJADORAS

El presente apartado aborda las cuestiones planteadas habitualmente ante la AEPD en relación con el tratamiento de datos personales por parte de los sindicatos y de la representación legal y sindical de las personas trabajadoras, en las materias que se indican.

1. TRATAMIENTO DE DATOS POR PARTE DE LOS REPRESENTANTES DE LAS PERSONAS TRABAJADORAS

El cumplimiento de las obligaciones y el ejercicio de los derechos de los representantes de las personas trabajadoras permiten el tratamiento de datos personales de las personas trabajadoras sin el consentimiento de éstas.

No obstante, este tratamiento cuenta con una serie de **límites**:

1. Sólo podrán ser objeto de tratamiento los **datos necesarios** para el ejercicio de esas funciones de representación.

> **Ejemplo.**
> No es admisible el tratamiento de datos privados de la persona trabajadora, como el número de teléfono personal. Sí lo sería, en cambio, la identificación de las personas trabajadoras que ocupan cada puesto de trabajo con nombre y apellidos (STS 572/2018 de 7 de febrero, Sala de lo Social) y también la dirección de correo electrónico corporativo.

2. El empleador no debe ceder a los representantes más datos de los **imprescindibles** para realizar sus funciones (**minimización de datos**).

> **Ejemplo.**
> El derecho a la protección de datos es contrario a una petición masiva de datos sobre las personas trabajadoras cuando los sindicatos no acrediten una «necesidad debidamente justificada» y no se especifique la finalidad para la que se requieren tales datos (Auto del TC 29/2008, de 28 enero). Por tanto, se vulnera el derecho a la protección de datos cuando, en el marco de un despido colectivo, no sólo se comunica a los representantes el nombre, la antigüedad o la categoría de la persona trabajadora, sino otra información innecesaria, como el número de DNI o el domicilio.
>
> En relación con el salario, la STS de 19 de febrero de 2009, Sala de lo Social, concluyó que la información de los salarios por categorías y departamentos,… cumple suficientemente con las exigencias que al respecto establece el artículo 1 de la Ley 2/1991 (RCL 1991, 39) , de enero, que regula los derechos de información de los trabajadores en materia de contratación, en cuanto dispone este precepto que "con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del DNI, el domicilio, el estado civil y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 mayo (RCL 1982, 1997), pudiera afectar a la intimidad personal", sin que el convenio colectivo de empresa aplicable amplíe

en esta materia los derechos establecidos en dicha Ley, y sin que el Sindicato demandante haya expuesto algún tipo de concreta justificación, que hiciera necesario el conocimiento de los datos solicitados en relación con el ejercicio de las funciones que constitucionalmente tiene reconocidas».

Respecto del absentismo, la empresa deberá informar sobre las causas y consecuencias de las bajas por incapacidad temporal (IT), pero no de las patologías médicas concretas de las personas trabajadoras que, por otra parte, tampoco debería conocer la empresa.

3. Los datos no podrán ser utilizados con **finalidades distintas** a las del ejercicio de las tareas representativas.

4. Siempre que los representantes de las personas trabajadoras hagan uso de los medios proporcionados por la empresa para el ejercicio de sus funciones, se les considerarán aplicables las políticas de seguridad de la entidad, tanto para el trabajo en los locales de la entidad, como en situación de movilidad o teletrabajo. Al tratarse de funciones distintas de las que llevan a cabo como usuarios en la empresa, tendrían que recibir perfiles específicos para acceder a los sistemas de información para el ejercicio de su acción representativa y recibir la formación adecuada para su manejo.

Como responsables del tratamiento en el desarrollo de su acción representativa, deberán cumplir las medidas de seguridad aplicables y, en particular, en el caso de que se produzca una brecha de seguridad que afecte a los tratamientos de datos de carácter personal realizados en el desempeño de sus funciones, tendrán que cumplir con los requisitos relativos a la notificación de quiebras de seguridad a la autoridad de control y, dependiendo de su alcance, a los afectados. En cualquier caso, deberán comunicarlo de forma inmediata a la empresa en la que desempeñen sus funciones.

5. Los convenios colectivos, en los términos previstos en el art. 64.9 del ET, podrían ser base jurídica para la lícita cesión de datos personales a los representantes de las personas trabajadoras.

> «Respetando lo establecido legal o reglamentariamente, en los convenios colectivos se podrán establecer disposiciones específicas relativas al contenido y a las modalidades de ejercicio de los derechos de información y consulta previstos en este artículo, así como al nivel de representación más adecuado para ejercerlos» (art.64.9 del ET).
>
> El art. 88.1 del RGPD prevé, igualmente, esta habilitación en los siguientes términos: «Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleadores o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral».

6. El tratamiento de datos requiere cumplir la obligación de **informar** a las personas trabajadoras.

7. Los representantes deben respetar la **confidencialidad** de esos datos.

2. PUBLICACIÓN DE DATOS PERSONALES EN TABLONES DE ANUNCIOS

El art. 81 del ET y la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical (LOLS), reconocen el derecho de los representantes unitarios y sindicales a disponer de un **tablón de anuncios** que permita facilitar información que pueda interesar a las personas trabajadoras y, en el caso del tablón de anuncios de los delegados y secciones sindicales, a los afiliados al sindicato.

> «En las empresas o centros de trabajo, siempre que sus características lo permitan, se pondrá a disposición de los delegados de personal o del comité de empresa un local adecuado en el que puedan desarrollar sus actividades y comunicarse con los trabajadores, así como uno o varios tablones de anuncios" (art. 81 del ET).
>
> "Con la finalidad de facilitar la difusión de aquellos avisos que puedan interesar a los afiliados al sindicato y a los trabajadores en general, la empresa pondrá a su disposición un tablón de anuncios que deberá situarse en el centro de trabajo y en lugar donde se garantice un adecuado acceso al mismo de los trabajadores» (art. 8.2 de la LOLS).

La publicación de notas informativas, anuncios, convocatorias, declaraciones e incluso sentencias en este tipo de tablones constituye una práctica habitual. La evolución tecnológica ha dado lugar a **tablones *online***. Cuando esas notas, anuncios o documentos contienen datos personales, la simple publicación constituye un tratamiento que puede comportar el acceso a datos por terceros carentes de legitimación.

Ejemplo.
No es admisible la publicación en internet con acceso libre de un censo electoral (SAN 4402/2013 de 18 de octubre, Sala de lo Contencioso).

"El derecho a la libertad sindical (…) ha de prevalecer sobre el derecho a la protección de datos personales, cuando, como sucede en el caso examinado, la acción sindical ampara la actuación del sindicato recurrente para divulgar entre los trabajadores de los centros los datos precisos, y únicamente necesarios, para el entendimiento de la noticia, teniendo un conocimiento cierto de la información relevante desde el punto de vista sindical" (SAN 5589/2007, de 19 de diciembre, Sala de lo Contencioso).

Ello obliga a tener en cuenta una serie de aspectos con el fin de aplicar adecuadamente las normas y garantizar los derechos de las personas concernidas:

- Será **responsable del tratamiento** quien sitúa materialmente la información en el tablón de anuncios.
- Sólo los **usuarios legitimados** deben tener acceso al tablón de anuncios.

Ejemplo.
Un tablón del que se pueda obtener información sindical no puede ubicarse en una zona de acceso libre para clientes o proveedores.

- Es fundamental que los tablones online se sitúen en la intranet de la empresa, nunca en Internet, salvo que únicamente resulten accesibles mediante usuario y contraseña (SAN 3578/2019, de 8 de junio, Sala de lo contencioso).

- Debe tenerse muy en cuenta el **principio de minimización** desde el punto de vista de la proporcionalidad de los tratamientos y de su finalidad.

> **Ejemplo.**
> La información publicada debería limitarse a la estrictamente necesaria. Como regla general, no es lícita la publicación íntegra de una determinada resolución administrativa o una sentencia judicial, sino que debe procederse a la anonimización de los datos personales no necesarios para el fin pretendido.

- Deben implementarse medidas para **impedir** el acceso a la información que proporcionan los tablones de anuncios a **terceros no autorizados**, salvo que prevalezcan las libertades de expresión e información propias de la libertad sindical (SAN 3094/2014, de 12 de junio, Sala de lo Contencioso).

> **Ejemplo.**
> Es contrario a la protección de datos la publicación durante un año en la web de un sindicato, de acceso ilimitado, de los nombres y apellidos de las personas trabajadoras contratados en sustitución de huelguistas acompañada del calificativo «esquiroles» (SAN 378/2013, de 8 de febrero, Sala de lo Contencioso).

3. ACCESO A DATOS POR LOS REPRESENTANTES DE LAS PERSONAS TRABAJADORAS

Distintas normas legales y reglamentarias laborales, entre ellas, el ET, atribuyen un amplio haz de facultades a los representantes de las personas trabajadoras y en particular al **comité de empresa y a los delegados sindicales (art. 10.3 de la LOLS**). En algunos casos el ejercicio de estas facultades puede comportar tratamientos de datos.

> **Ejemplo.**
> El comité de empresa tendrá derecho a ser informado de todas las sanciones impuestas por faltas muy graves, a recibir la copia básica de los contratos y la notificación de las prórrogas y de las denuncias correspondientes a los mismos en el plazo de diez días siguientes a que tuvieran lugar y también a ser informados de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles (art. 64 del ET). Los delegados sindicales tienen derecho a ser oídos por la empresa previamente a la adopción de medidas de carácter colectivo que afecten a los trabajadores en general y a los afiliados a su sindicato en particular, y especialmente en los despidos y sanciones de estos últimos. (art. 10.3.3º de la LOLS).

No obstante, este acceso potencial a datos personales debe estar regido por el cumplimiento estricto de los principios de protección de datos:

- Únicamente podrán comunicarse datos cuando resulte **estrictamente necesario** para el cumplimiento de los deberes que el ET establece para la empresa. En este marco, no hace falta el consentimiento de la persona trabajadora para entregar la copia básica del contrato.

En todos aquellos casos en los que la información pueda presentarse de modo estadístico o anonimizado permitiendo al comité cumplir con sus funciones se optará por este método. No se justifica que los representantes conozcan el domicilio particular de las personas trabajadoras, por ejemplo, para enviar propaganda electoral. En cambio, sí estaría justificado acceder a la lista de miembros de una bolsa de empleo (STS 5761/2015, de 21 de diciembre, Sala de lo Social).

- Los **destinatarios de la información** serán los previstos por la norma que habilite la comunicación de datos.

- Los representantes unitarios y sindicales que acceden a información de las personas trabajadoras están obligados a guardar **secreto** y al cumplimiento de los principios de la normativa de protección de datos. La información no podrá ser utilizada para **fines diferentes** de aquellos que se derivan de la legislación laboral, y que entroncan, en este caso, con la constatación de que el empleador cumple las exigencias legales y convencionales correspondientes en materia de condiciones de trabajo y empleo.

«Los miembros del comité de empresa y este en su conjunto, así como, en su caso, los expertos que les asistan deberán observar el deber de sigilo con respecto a aquella información que, en legítimo y objetivo interés de la empresa o del centro de trabajo, les haya sido expresamente comunicada con carácter reservado.

En todo caso, ningún tipo de documento entregado por la empresa al comité podrá ser utilizado fuera del estricto ámbito de aquélla ni para fines distintos de los que motivaron su entrega. El deber de sigilo subsistirá incluso tras la expiración de su mandato e independientemente del lugar en que se encuentren» (arts. 65.2 y 65.2 del ET).

En relación con la **copia básica**, la STC 142/1993 aclaró que el conocimiento por parte de los representantes de cierta información personal (importe de la retribución, datos personales que aparecen en el contrato, etc.) no vulnera al derecho a la intimidad, máxime cuando esa "copia" no puede contener los datos personales que expresamente excluye el art. 8.4 del ET. La persona trabajadora puede negarse a que datos ajenos a la relación de trabajo, como la situación familiar, aparezcan en la copia básica.

«Con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del documento nacional de identidad o del número de identidad de extranjero, el domicilio, el estado civil, y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pudiera afectar a la intimidad personal. El tratamiento de la información facilitada estará sometido a los principios y garantías previstos en la normativa aplicable en materia de protección de datos» (art. 8.4 del ET).

Por tanto, la copia básica no habilita la comunicación de todos los datos de la persona trabajadora, sino únicamente de aquellos que permiten desempeñar la **función de control** asignada a la representación de las personas trabajadoras.

Respecto de la **entrega de documentos de cotización** (Relación Nominal de Trabajadores o RNT –antiguo TC2- y el documento de Relación de Liquidación de Cotizaciones o RLC –antiguo TC1-) al **comité de empresa**, debe tenerse en cuenta lo siguiente:

- El comité debe actuar en el **marco de las funciones** que le atribuye el ET y demás normas legales y reglamentarias.
- El tipo de información que el empleador debe suministrar es **limitado**, y no alcanza a las nóminas de las personas trabajadoras.
- El **convenio colectivo** podría contener previsiones específicas, pues al ser fuente reguladora de la relación laboral podría ampliar el ámbito de la cesión.
- Los representantes **no pueden publicar** estos documentos en un tablón de anuncios de la empresa.

4. DESCUENTO DE LA CUOTA SINDICAL

El art. 9.1 del RGPD prohíbe el tratamiento de datos personales que revele la afiliación sindical, dato personal que se encuadra entre las categorías especiales. No obstante, el art. 9.2 del RGPD contiene excepciones respecto de esa prohibición.

Concretamente la recogida en su apartado d), dentro de las actividades legítimas del sindicato, y siempre con el consentimiento de la persona afiliada, el sindicato puede proceder a la comunicación del dato de afiliación a la empresa a efectos del descuento de la cuota sindical.

En este marco, en el preámbulo de la LOPDGDD se aclara que es lícito el tratamiento de datos personales por parte de la empresa relativo a la afiliación sindical con la finalidad de **descuento de la cuota sindical**.

> «La prestación del consentimiento no dará cobertura a la creación de "listas negras" de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea».

El tratamiento de datos sobre la afiliación sindical por el empleador es lícito «**cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado** en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado» (art. 9.2.b del RGPD).

La legislación española exige en todo caso el **consentimiento de la persona trabajadora a efectos del descuento de la cuota sindical**.

«El empresario procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de éste» (art. 11.2 de la LOLS).

Por tanto, en este marco, el consentimiento es necesario para que el sindicato pida a la empresa el descuento de la cuota.

Una vez obtenido el consentimiento para ese tratamiento, las siguientes operaciones:

- que la empresa comunique al sindicato las personas trabajadoras a las que corresponden las cuotas que ingresa, así como los datos del pago y

- que la empresa informe al sindicato sobre las cuotas impagadas identificando a la persona trabajadora concreta,

tienen su base jurídica en el cumplimiento de una obligación legal por el responsable.

El tratamiento de estos datos requiere la adopción de **procedimientos** para proteger información particularmente sensible:

a) Es recomendable disponer de procedimientos de captación del consentimiento como impresos o modelos de solicitud en los que la persona trabajadora autorice por escrito el tratamiento.

b) Debe limitarse el uso de estos datos a la finalidad para la que se han recabado (cobrar la cuota y transferir las cantidades a la organización sindical).

Ejemplo.
No es posible tratar el dato de afiliación sindical con la finalidad de practicar descuentos en el salario a los afiliados del sindicato convocante de una huelga (STC 11/1998).

5. COMUNICACIONES POR CORREO ELECTRÓNICO

El envío de **información sindical a través del correo electrónico** implica un tratamiento de datos personales, pues una dirección electrónica es un dato personal. El Tribunal Constitucional ha señalado que el envío de este tipo de mensajes de correo electrónico constituye un derecho de los representantes amparado por el derecho fundamental de libertad sindical (STC 281/2005), de modo que los representantes podrían utilizar la infraestructura de la empresa, que a su vez debería proporcionarles la dirección de correo electrónico de las personas trabajadoras. No obstante, deben darse ciertas condiciones, como que la empresa disponga del servicio de correo electrónico corporativo, que los envíos se realicen de modo proporcional y que no se perjudique el **normal funcionamiento de la organización**.

Cuando se den las circunstancias anteriores, existirá legitimación para que se produzca una comunicación de datos personales a los representantes. Sin embargo, deben tenerse en cuenta las siguientes consideraciones:

1. Existen **procedimientos automatizados** que permiten satisfacer el derecho a la libertad sindical sin necesidad de realizar una cesión de datos personales.

Ejemplo.
La utilización de listas de distribución permite que el sindicato remita la información a una dirección corporativa del tipo listasindical@empresa.es, sin acceso a los datos. Además, puede incorporarse la información exigida por el RGPD en los pies de los correos y automatizar la supresión y la oposición a los tratamientos mediante las bajas en las listas a petición del usuario.

2. La comunicación de datos se limitará a los **estrictamente necesarios**.

> **Ejemplo.**
> En ningún caso se cederán datos como la dirección de cuentas privadas de la persona trabajadora, sólo la dirección de correo electrónico corporativa.

3. El dato se utilizará para la **finalidad** para la que fue comunicado.

4. El sindicato está obligado a cumplir con las previsiones del **RGPD y de la LOPDGDD**.

5. El sindicato debe respetar el **derecho de oposición** de los trabadores, salvo en el supuesto de elecciones sindicales, momento en el cual prevalece la libertad sindical respecto del derecho a la protección de datos.

La celebración de **elecciones sindicales** legitima las comunicaciones de los datos censales necesarios para permitir al sindicato remitir información electoral y participar en el proceso electoral.

6. VIOLENCIA DE GÉNERO Y ACOSO EN EL TRABAJO

Los representantes de las personas trabajadoras únicamente podrán conocer la identidad de las mujeres supervivientes **a la violencia de género** cuando sea imprescindible para el ejercicio de sus labores de representación. El principio de minimización de datos exige que sea necesario que los representantes conozcan la identidad de la víctima.

> **Ejemplo.**
> Negativa del empleador a acceder a una reconfiguración del tiempo de trabajo de una mujer superviviente a la violencia de género. Para comprobar las razones alegadas por el empleador es posible que deba proporcionarse información que permita identificar a la superviviente, como, por ejemplo, el puesto de trabajo desempeñado.

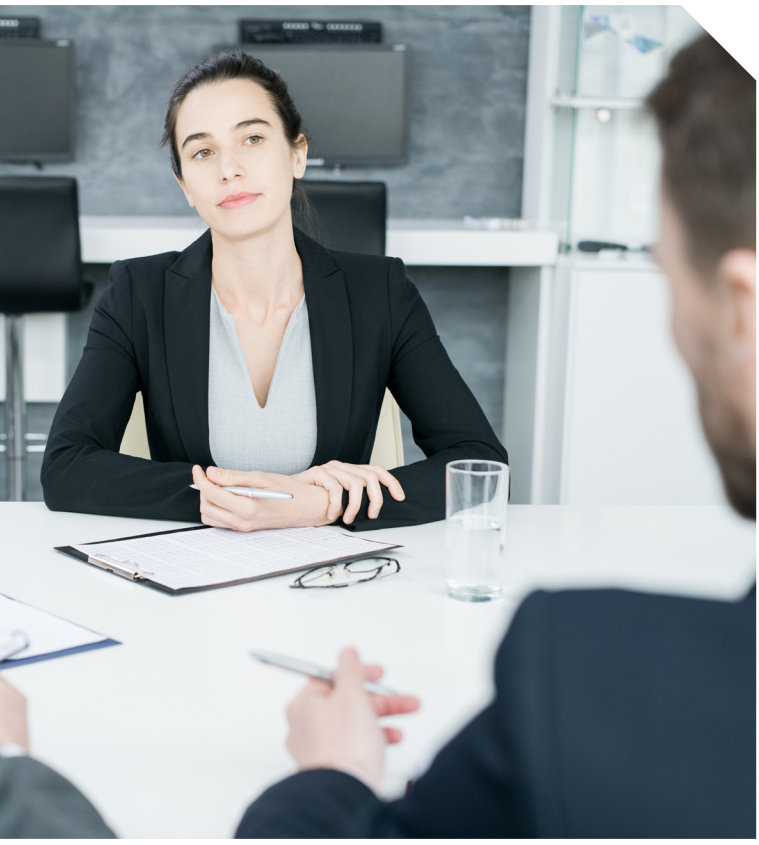
La misma regla debe aplicarse en **supuestos de acoso**. En estas situaciones la necesidad de conocer la identidad de la víctima y del presunto acosador por parte de los representantes puede resultar imprescindible y más fácil de demostrar.

> **Ejemplo.**
> Además de recibir información sobre las faltas muy graves (art. 64 del ET), los representantes deben ser oídos en caso de imposición de sanciones por faltas graves o muy graves a otros representantes (art. 68 del ET) o a afiliados al sindicato (art. 10.3.3 de la LOLS), por lo que, si el acosador es un representante de las personas trabajadoras, el resto de los representantes necesariamente deben ser informados sobre esas actuaciones y participar en ellas.

Se proporciona más información sobre este tema en el apartado 4, punto 14 de esta Guía y en las Recomendaciones de la AEPD sobre la Protección de Datos como garantía en las políticas de prevención del acoso.

7. PERÍODOS DE CONSULTAS (TRASLADOS, MODIFICACIONES SUSTANCIALES DE CONDICIONES DE TRABAJO, SUSPENSIONES Y DESPIDOS COLECTIVOS)

El ET y el Reglamento de los procedimientos de despido colectivo y de suspensión de contratos y reducción de jornada, aprobado por Real Decreto 1483/2012, de 29 de octubre, exigen que el empleador y los representantes de las personas trabajadoras celebren un **período de consultas** antes de la adopción de determinadas decisiones con impacto en las personas trabajadoras, como el traslado (art. 40 del ET), la modificación sustancial de condiciones de trabajo (art. 41), la transmisión de empresa (art. 44), la suspensión de contratos (art. 47), el despido colectivo (art. 51) o la inaplicación del convenio colectivo (art. 82).



El período de consultas es una auténtica negociación y la ley exige que el empleador proporcione a los representantes la información pertinente para que conozcan la situación y las razones de la empresa.

Esa información puede incluir **datos personales** de las personas trabajadoras, como su **nombre y apellidos y el puesto** que ocupan. Además, debe informarse sobre los criterios que el empleador pretende utilizar para seleccionar a las personas trabajadoras afectadas por la medida, como pueden ser la **edad**, la **antigüedad** o la **productividad**, dependiendo del caso. Este tratamiento de datos debe respetar el principio de **minimización**, por lo que el empleador no ha de proporcionar datos que no sean necesarios a estos efectos, y los representantes de las personas trabajadoras no pueden utilizar los datos con otra finalidad incompatible.

Además, ambas partes deben respetar la **confidencialidad** de los datos personales, por lo que la difusión de las negociaciones en tiempo real o su **grabación** requieren el **consentimiento** de los afectados.

Las personas trabajadoras, por su parte, tienen derecho a **impugnar la decisión empresarial** y para ello pueden **conocer los motivos** que han llevado a su adopción. A tal fin, la persona trabajadora tiene derecho a solicitar el **baremo y los criterios** utilizados a través del derecho de información sobre el tratamiento de sus datos personales (resolución AEPD R/01656/2013).

7. VIGILANCIA DE LA SALUD

1. BASES JURÍDICAS PARA EL TRATAMIENTO DE DATOS

La LPRL y sus normas de desarrollo imponen a la empresa la realización de un conjunto de actividades cuyo fin último es **evitar o disminuir los riesgos derivados del trabajo**. Para esta tarea resulta necesario tratar datos personales de las personas trabajadoras.

Ejemplo.
La planificación de la prevención obliga, como mínimo, a disponer de una relación detallada de los puestos de trabajo y de las personas que los ocupan. Además, deben identificarse y evaluarse los riesgos específicos del puesto, ligados en muchas ocasiones a las características personales o de salud de la propia persona trabajadora. ¿Es alérgico a determinados elementos químicos? ¿Necesita ciertas condiciones de luminosidad o de tamaño de letra en la pantalla de su ordenador? ¿Es capaz de identificar con claridad una alarma acústica?

El tratamiento de datos personales en materia de prevención de riesgos se encuentra legitimado por la existencia de una relación contractual cuyo cumplimiento, desarrollo y control lo hace necesario. El **contrato de trabajo**, en combinación con el **cumplimiento de las obligaciones legales** establecidas en el ET y en la LPRL, son las **bases jurídicas** del tratamiento de datos.

El art. 9.2 .h) del RGPD admite la recogida y tratamiento de datos con fines de «**medicina preventiva o laboral**» y «**evaluación de la capacidad laboral del trabajador**», sin perjuicio de que han de respetarse las garantías y límites pertinentes en relación con los datos que se pretenden obtener y su posible uso posterior.

Una de las obligaciones principales del empleador en el campo de la prevención de riesgos laborales es la **vigilancia en la salud** de las personas trabajadoras. Es una obligación que no implica un deber correlativo para las personas trabajadoras, pues los reconocimientos médicos a cargo del empleador son, con carácter general, **voluntarios** para aquéllas, que deben prestar su **consentimiento**.

«El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo. Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento» (art. 22.1 de la LPRL).

Esta vigilancia de la salud puede ser **obligatoria** conforme al artículo 22.1 de la LPRL, previo informe de los representantes de las personas trabajadoras, en los siguientes supuestos:

1. Reconocimientos **imprescindibles** para evaluar los efectos de las condiciones de trabajo sobre la salud de las personas trabajadoras.

2. Verificación de si el estado de salud de la persona trabajadora puede constituir un **peligro** para ella misma, para las demás personas trabajadoras, o para otras relacionadas con la empresa.

3. Obligación legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad.

Tanto si el reconocimiento médico es voluntario como si es obligatorio, la **base jurídica** para el tratamiento de datos personales derivados de esa vigilancia de la salud no sería el consentimiento, sino la **ejecución del contrato de trabajo** (art. 6.1.b) del RGPD) y el cumplimiento de las obligaciones legales en materia de prevención, como se ha indicado. No obstante, no debe olvidarse que:

- El cumplimiento del **deber de información** es esencial, tanto en relación con los resultados de la vigilancia de la salud (art. 22.3 de la LPRL) como respecto del tratamiento de datos.

- Hay que prestar particular atención al **principio de proporcionalidad**, de modo que sólo cabe recabar y utilizar los datos estrictamente necesarios para la finalidad de prevención.

El reconocimiento debe vincularse a la **aptitud laboral**, sin que pueda proporcionar al empleador ningún otro tipo de información:

1. Los datos de los que el empleador puede disponer, y que son susceptibles de tratamiento, deben ser **datos necesarios** para la correcta ejecución del contrato.

> **Ejemplo.**
> En el caso de que el reconocimiento médico permita averiguar datos no vinculados estrictamente con la aptitud laboral, como el consumo de drogas, debe obtenerse previamente el consentimiento informado de la persona trabajadora (STC 196/2004, de 15 de nov).

> Recogiendo la doctrina constitucional, la STSJ CAT 12721/2012, de diciembre, Sala de lo Social, considera lesionado el derecho a la intimidad de una persona trabajadora a la que se le realizó una analítica para comprobar la presencia o no del VIH, sin su conocimiento, a la que sólo se le informa de la práctica de la empresa para efectuar un reconocimiento médico, y sin que se prestase consentimiento expreso, agravado por la posterior divulgación del resultado positivo al director médico y al director general adjunto de la empresa.

2. El empleador **no está legitimado para conocer el concreto diagnóstico médico**, de modo que sólo podrá acceder a las conclusiones de dicha vigilancia de la salud referidas al concepto de «apto» o «no apto», o al desglose de las tareas que es posible realizar, con las recomendaciones pertinentes sobre la adaptación o el cambio de puesto.

> *"Si lo que debe protegerse ante todo es la confidencialidad de la información sanitaria relativa a los trabajadores, no tiene sentido afirmar que cabe comunicar a los empresarios cualquier dato que exceda de la mera "conclusión" sobre la idoneidad del trabajador para el puesto de trabajo; es decir, la mutua sólo puede decir al empresario si reputa apto al trabajador, sin proporcionarle ninguna otra información adicional"* (STS 6351/2009, de 20 de octubre, Sala de lo Contencioso).

3. La empresa no tiene derecho a conocer datos de salud más específicos incluso cuando se refieran a una **persona trabajadora especialmente sensible a los riesgos derivados del trabajo** (por ejemplo, trabajadoras embarazadas, o personas con capacidades diferentes).

«El empresario garantizará de manera específica la protección de los trabajadores que, por sus propias características personales o estado biológico conocido, incluidos aquellos que tengan reconocida la situación de discapacidad física, psíquica o sensorial, sean especialmente sensibles a los riesgos derivados del trabajo. A tal fin, deberá tener en cuenta dichos aspectos en las evaluaciones de los riesgos y, en función de éstas, adoptará las medidas preventivas y de protección necesarias» (art. 25.1 de la LPRL).

Conviene insistir en que **las empresas sólo pueden tener conocimiento de las conclusiones derivadas de los reconocimientos**, en relación con la aptitud de la persona trabajadora para el desempeño de su puesto. El servicio de prevención deberá remitir a la empresa las conclusiones que se deriven de los reconocimientos efectuados y en relación con la aptitud de la persona trabajadora para el puesto desempeñado.

Ejemplo.
Esta conclusión se extiende a cualesquiera tratamientos de datos vinculados con la prevención de riesgos laborales, como por ejemplo la comunicación de datos que sea necesaria para cumplir las obligaciones de coordinación cuando en un mismo centro de trabajo desarrollen su actividad personas trabajadoras de varias empresas, en los términos del art. 24 de la LPRL.

Los datos médicos de las personas trabajadoras de una empresa que forma parte integrante de un grupo empresarial, que tiene organizado sus servicios médicos de prevención como autónomos de la empresa matriz del grupo, no puede permitir que los servicios médicos de dicha empresa matriz puedan acceder a los datos de los trabajadores/as de todas las empresas del grupo y si ese acceso se encuentra justificado por el hecho de que algunas de las personas trabajadoras de las empresas filiales trabajen de forma continuada en la central o porque alguno de los trabajadores/as puedan eventualmente asistir a reuniones de trabajo en las instalaciones centrales de la empresa matriz, fuera de los supuestos legalmente permitidos y, en todo caso, tomando siempre como interés preferente la salud del paciente. Las condiciones de seguridad de la aplicación que permitía el acceso no autorizado a datos médicos a terceros no autorizados supusieron el incumplimiento de las medidas de custodia y seguridad necesarias (SAN 4419/2011, de 6 de octubre, Sala de lo Contencioso).

Por otro lado, en el ámbito laboral, también se producen formas de violencia digital, en numerosas ocasiones acompañadas de conductas constitutivas de acoso laboral y acoso sexual o por razón de sexo. Estas conductas afectan a la salud física, psíquica y emocional de las personas trabajadoras, por lo que combatirlas es una obligación del empleador, garante de la salud y seguridad de las personas trabajadoras. Más información en las Recomendaciones de la AEPD sobre el acoso digital.

En todo caso, el RGPD permite el tratamiento de datos personales de salud sin consentimiento del afectado en situaciones de interés público en el ámbito de la salud pública y en el cumplimiento de obligaciones legales en el ámbito laboral derivado de dichas situaciones. Véase el espacio de la web de la AEPD sobre "Protección de datos y coronavirus".

Se puede completar la información con la **Guía para pacientes y usuarios de la sanidad**

2. EL ACCESO A LOS DATOS POR LA EMPRESA Y LOS DELEGADOS DE PREVENCIÓN

La legislación de prevención de riesgos laborales admite en ciertos casos las **comunicaciones de datos personales**. Así, la legislación legitima y obliga a comunicar datos a los delegados de prevención, a la autoridad sanitaria en el marco de la Ley 14/1986, de 25 de abril, General de Sanidad, a la Inspección de Trabajo y Seguridad Social o a la autoridad laboral, sin olvidar la comunicación de datos que requieran los jueces y tribunales, o las necesarias en caso de urgencia médica o en estudios epidemiológicos.

Los casos que plantean mayores dificultades son los que se refieren al **acceso a información por la propia empresa y por los delegados de prevención**.

Las facultades de acceso a la información por parte de la empresa son muy limitadas y en la práctica se refieren a conocer las condiciones de aptitud o no aptitud de la persona trabajadora. El tratamiento por parte de los servicios de prevención de riesgos laborales del historial médico, consecuencia de los reconocimientos médicos realizados a las personas trabajadoras, deberá limitarse a las previsiones del artículo 22.4 de la LPRL. Por tanto, ese precepto **impide el acceso a la información médica obtenida al amparo de lo dispuesto en la LPRL por parte del empleador o de cualquier tercero**, incluidas las personas u órganos con responsabilidades en materia de prevención, distintos del «personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores», **con la única excepción de las conclusiones** derivadas de dicho seguimiento en cuanto a la **aptitud de las personas trabajadoras** para el desempeño del puesto de trabajo.

Cuando la vigilancia de la salud es realizada por **facultativos externos**, los médicos de empresa no tienen acceso al diagnóstico médico, pues se produciría una comunicación de datos sin consentimiento de la persona trabajadora. Todo ello sin perjuicio de la posible comunicación a los órganos jurisdicciones o cuando concurra un riesgo para terceros en los términos previstos en la ley.

No obstante, es posible que el empleador deba acceder de modo específico a datos personales de la persona trabajadora necesarios para el cumplimiento de sus obligaciones que desborden la calificación de apto o no apto. En tales casos, la legitimación para el tratamiento deriva de la propia regulación, pero se limitará a los datos estrictamente necesarios.

Ejemplo.
Es evidente que si debe adaptarse una pantalla de ordenador con un determinado tamaño de letra existirán problemas visuales, si se debe cambiar un avisador acústico por uno visual existen problemas de audición y que, si el uniforme de trabajo debe ser de un determinado tejido, puede existir una alergia. En todos estos casos puede deducirse la presencia de una discapacidad o enfermedad.

Con carácter general, el **consentimiento no es una base jurídica** que justifique la cesión de datos médicos, pues la persona trabajadora no tiene completa libertad para prestar ese consentimiento. Y, desde luego, **tampoco es base jurídica el convenio colectivo**.

"Las previsiones del Convenio en esta materia, si se entienden referidas al contenido de los reconocimientos, no se ajustan a las exigencias derivadas del respeto a la intimidad y esta invasión de la intimidad no puede justificarse en el presente caso en función del consentimiento del trabajador. En primer lugar,

porque no hay ningún interés general que justifique el que se recaben estos reconocimientos médicos confidenciales, se hagan constar en una tarjeta profesional y se remitan a un organismo paritario -la Fundación Laboral Construcción- que no tiene una configuración técnico-sanitaria. La remisión de estos datos carece de interés en términos tanto sanitarios, como de prevención, pues lo importante es que los reconocimientos se realicen y que sus conclusiones se tengan en cuentan por el empresario y los órganos competentes en materia de prevención para adoptar las medidas de protección oportunas, lo que ninguna relación tiene con la remisión de esos reconocimientos a un organismo paritario sin ninguna finalidad específica en orden a la adopción de medidas preventivas en atención al contenido de los reconocimientos y muchos menos con la mera circulación de esa información en una tarjeta profesional. La única función a la que parece apuntar esa ruptura de la confidencialidad a través de la circulación de los reconocimientos sería el objetivo de evitar la repetición de los informes en caso de rotación [artículo 130 d) del Convenio], lo que es contrario a la doctrina de la STC 70/2009. En segundo lugar, porque el consentimiento del trabajador a la hora de proporcionar esta información puede verse perturbado por las consecuencias que la negativa a aportar los informes pueda tener sobre sus posibilidades de ser contratado a partir de la posible clasificación de los trabajadores distinguiendo entre quienes aportan los reconocimientos y los que no lo hacen" (STS 6234/2010, de 27 de octubre, Sala de los Social).

Por su parte, los miembros del Comité de Seguridad y Salud y los **delegados de prevención** pueden acceder a la información necesaria para el ejercicio de sus funciones y, en particular, a la prevista en los arts. 18, 23 y 36 de la LPRL.

«c) Ser informados por el empresario sobre los daños producidos en la salud de los trabajadores una vez que aquél hubiese tenido conocimiento de ellos, pudiendo presentarse, aún fuera de su jornada laboral, en el lugar de los hechos para conocer las circunstancias de los mismos.

d) Recibir del empresario las informaciones obtenidas por éste procedentes de las personas u órganos encargados de las actividades de protección y prevención en la empresa, así como de los organismos competentes para la seguridad y la salud de los trabajadores, sin perjuicio de lo dispuesto en el artículo 40 de esta Ley en materia de colaboración con la Inspección de Trabajo y Seguridad Social» (art. 36.2 de la LPRL).

La información resultante de las acciones de vigilancia de la salud del art. 22 de la LPRL sólo autoriza al empleador, y en su caso a terceros ajenos a los profesionales médico-sanitarios que practicaron las pruebas de reconocimiento, a conocer el dato de apto o no apto para el desempeño del puesto de trabajo que ocupa la persona trabajadora o el pretenda asignársele, de modo que los delegados de prevención podrán conocer este extremo y no todo el expediente médico-laboral de la persona trabajadora.

En consecuencia, podrán acceder a datos personales sobre daños en la salud de las personas trabajadoras cuando tengan su origen en un hecho relacionado con el entorno laboral, sólo para la **finalidad de control** que les atribuye la LPRL y únicamente procederá el tratamiento de los **datos estrictamente necesarios**, entendiendo por tales los relativos a la gravedad y naturaleza de los daños. El delegado de prevención está vinculado a los principios de protección de datos personales y debe respetar el deber de confidencialidad.

«A los Delegados de Prevención les será de aplicación lo dispuesto en el apartado 2 del artículo 65 del Estatuto de los Trabajadores en cuanto al sigilo profesional debido respecto de las informaciones a que tuviesen acceso como consecuencia de su actuación en la empresa» (art. 37.3 LPRL).

«2. Los miembros del comité de empresa y éste en su conjunto, así como, en su caso, los expertos que les asistan deberán observar el deber de sigilo con respecto a aquella información que, en legítimo y objetivo interés de la empresa o del centro de trabajo, les haya sido expresamente comunicada con carácter reservado» (art. 65.2 del ET).

Para obtener más información sobre situaciones excepcionales como la pandemia de la COVID 19 se puede consultar el espacio de la web de la AEPD sobre "Protección de datos y coronavirus".

En suma, los delegados de prevención, respetando las exigencias de **confidencialidad** impuestas por la legislación de protección de datos, pueden acceder a los **informes y documentos resultantes de la investigación de los accidentes de trabajo y enfermedades profesionales** que lleve a cabo la empresa, en particular, cuando la información se encuentre incorporada en documentos técnicos y prolijos (STSJ CANT 862/2005, de 1 de junio, Sala de lo Social), ya que:

- El derecho de información de los delegados de prevención tiene la **misma extensión que la potestad informativa de la autoridad laboral** en este ámbito.
- La investigación de accidentes de trabajo y enfermedades profesionales forma parte del proceso de **evaluación de los riesgos laborales** y el acceso a sus resultados deriva del derecho de información sobre la evaluación de riesgos reconocido en el art. 23 de la LPRL (STS 912/2016, de 24 febrero 2016, Sala de lo Social).

Finalmente, el art. 39.2.b) de la LPRL permite al **Comité de Seguridad y Salud** «conocer cuantos documentos e informes relativos a las condiciones de trabajo sean necesarios para el cumplimiento de sus funciones, así como los procedentes de la actividad del servicio de prevención, en su caso».

3. TECNOLOGÍA WEARABLE (DISPOSITIVOS PONIBLES)

La monitorización de datos de salud a través de **dispositivos inteligentes**, como pulseras o relojes, está, por lo general, **prohibida, a menos que esté establecida por ley o reglamentariamente**, por las siguientes razones:

- No se enmarca en la **vigilancia de la salud** propia de la prevención de riesgos laborales.
- Supone el tratamiento de una categoría especial de datos (salud) **sin una base jurídica**.
- No cuenta con una **finalidad** legítima.
- Vulnera el principio de **proporcionalidad**, porque conlleva una monitorización permanente y permitiría al empleador acceder a datos de salud específicos, y no exclusivamente a la valoración sobre la aptitud de la persona trabajadora para desempeñar el trabajo.

Dada la relación desigual entre empresas y personas trabajadoras y la naturaleza sensible de los datos de salud, **las personas trabajadoras no son verdaderamente «libres» para consentir**, y por ello el consentimiento de la

persona trabajadora no es una base jurídica válida en estos casos. Incluso si el empleador utiliza a un tercero para recopilar los datos de salud, el tratamiento seguiría siendo ilícito, salvo que se acreditase un interés legítimo, una finalidad específica, una monitorización proporcional, o bien que se garantizase la anonimización completa de los datos.

Ejemplo.
Una organización ofrece a sus trabajadores/as dispositivos de seguimiento del estado físico como regalo. Los dispositivos cuentan el número de pasos que los trabajadores/as dan y registra sus latidos y patrones de sueño a lo largo del tiempo. Los datos de salud resultantes sólo deberían ser accesibles para el trabajador y no para el empresario. Cualquier dato transferido entre la persona trabajadora (como afectado) y el proveedor del dispositivo/servicio (como responsable del tratamiento) es una cuestión que compete a ambas partes. Habida cuenta de que los datos de salud también podrían ser objeto de tratamiento por la parte comercial que haya fabricado los dispositivos u ofrezca un servicio a los empresarios, el empresario, a la hora de elegir el dispositivo o servicio, debe evaluar la política de privacidad del fabricante y/o proveedor de servicios, con el fin de asegurarse de que no se produzca un tratamiento ilícito de los datos de salud de las personas trabajadoras (Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo del Artículo 29).

4. RELACIÓN EMPRESA-SERVICIO DE PREVENCIÓN

El desarrollo de tareas de prevención de riesgos supone la presencia de áreas de actuación especializadas (seguridad, ergonomía y psicosociología, higiene industrial, medicina y enfermería del trabajo) y de profesionales con perfiles y exigencias organizativas diversas. Hay que disponer **de medios y recursos adecuados** que no siempre se encuentran a disposición de todas las a empresas.

La relación entre la empresa y el servicio de prevención requerirá un tratamiento de datos, en concreto comunicaciones de datos relativos a las personas trabajadoras, que no exigen el consentimiento de éstas porque la **base jurídica** es una obligación legal, la prevención de riesgos laborales.

En relación con la comunicación de datos, se deben tener en cuenta sentencias como la SAN de 24 de mayo de 2007, Sala de lo Contencioso. La sentencia declara la nulidad de las sanciones impuestas por la AEPD a la mutua por usar datos de carácter personal objeto de tratamiento automatizado para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos, y por cesión de los datos de carácter personal, fuera de los casos en los que estén permitidas. La cesión de datos producida se encuentra amparada por la aplicación de los principios de racionalidad y de unidad de historias clínicas y tiene una finalidad legítima, la correcta aplicación de la normativa sobre Seguridad Social y Prevención de Riesgos Laborales y la prevención del fraude, por lo que no es exigible el consentimiento de la persona trabajadora denunciante.

La condición de **responsable del tratamiento** varía según se trate de un servicio de prevención propio, ajeno o mancomunado:

- Si se trata de un **servicio propio**, la empresa será responsable del tratamiento. En caso de servicio de prevención propio existirán en el seno de la empresa distintos perfiles y facultades de acceso a datos de salud. El servicio de prevención ajeno será responsable del tratamiento. En estos supuestos existe una total separación entre la empresa y el servicio de prevención. El servicio de prevención ajeno deberá limitarse a comunicar al empleador la condición de apto o no apto de la persona trabajadora o, en su caso, la necesidad de acometer adaptaciones o mejoras para reducir o eludir los riesgos. Cualquier otra comunicación de datos al empleador exige un interés legítimo del empleador.

- Los servicios de prevención mancomunados se pueden constituir entre empresas que desarrollan simultáneamente actividades en un mismo centro de trabajo, edificio o centro comercial. Dichos servicios, tengan o no personalidad jurídica diferenciada, tendrán la consideración de servicios propios de las empresas que los constituyan. Si el servicio de prevención mancomunado tiene personalidad jurídica propia, se considera como un servicio de prevención ajeno y, por tanto, responsable del tratamiento. Si el servicio de prevención mancomunado no tuviera personalidad jurídica independiente, las empresas, de la misma forma que en los casos de servicios de prevención propios, asumirían la condición de responsables del tratamiento.

La **confidencialidad** debe garantizarse plenamente, y por ello los **sistemas de información** para la gestión de servicios de prevención deberán tener en cuenta:

1. Implementar sistemas de registro o logs, a los efectos de verificar que los accesos se corresponden únicamente al personal habilitado. y debidamente autorizado.

2. Deberán definir de modo muy preciso los **perfiles de acceso** y las funciones de cada uno de los usuarios.

> **Ejemplo.**
> No pueden tener el mismo el perfil el administrativo que organiza las citas y el médico del trabajo. Del mismo modo, el responsable de la adaptación ergonómica de un puesto de trabajo debería poder acceder a los datos de salud que resulten necesarios para su actividad.

5. CAMBIO DEL SERVICIO DE PREVENCIÓN

La LPRL obliga al empleador a **garantizar a las personas trabajadoras a su servicio la vigilancia periódica de su estado de salud** en función de los riesgos inherentes al trabajo (art. 23) y, para cumplir esa tarea, le permite optar por designar una o varias personas trabajadoras, constituir un servicio de prevención propio o concertar con un servicio de prevención ajeno (arts. 30 y ss.).

Cuando se produce un cambio en el servicio de prevención, la comunicación de los datos relativos a la vigilancia de la salud de las personas trabajadoras a la nueva entidad que desarrolle el servicio de prevención sería un supuesto de comunicación de datos previsto en el artículo 23.1 de la LPRL, en relación con el art. 30.3, derivada de la obligación de puesta a disposición del nuevo servicio y de la obligación de mantenimiento de la historia clínico-laboral (art. 37.3.c) del Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención).

No obstante, este tratamiento de datos debe respetar los principios de **minimización** y de **limitación de la finalidad**, lo que supone:

- Que los datos de salud sólo pueden ser comunicados al nuevo servicio de prevención, y no a cualquier otra entidad.
- Que la comunicación debe producirse directamente entre los servicios médicos de las empresas de prevención involucradas.

Por consiguiente, vulnera el derecho a la protección de datos que el servicio de prevención que cesa entregue los datos **al empleador** para que éste se los haga llegar al nuevo servicio de prevención.

En todo caso, deben respetarse estas cautelas:

1. Los datos no pueden utilizarse con una **finalidad** distinta a la prevención de riesgos laborales.

2. La persona trabajadora tiene derecho a ser **informada**.

3. El servicio de prevención que cesa no debe proceder a la **supresión** de los datos inmediatamente, pues tiene obligación de **conservación**, en los términos previstos en la normativa laboral que resulte de aplicación.

Ejemplo.
El art. 9.3 del Real Decreto 665/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes cancerígenos durante el trabajo, obliga a conservar los historiales médicos durante cuarenta años después de terminada la exposición.

6. HISTORIA CLÍNICA DE LAS PERSONAS TRABAJADORAS

La **historia clínica** de las personas trabajadoras debe regirse, además de por lo previsto en la legislación de protección de datos, por los principios de la Ley 41/2002, 2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Al propio tiempo, de lo establecido en el párrafo segundo del artículo 22.4 de la LPRL se deriva el derecho del personal sanitario que realice las acciones de vigilancia de la salud al conocimiento de la información médica que se derive de la misma. En este sentido, dicha información compondrá, según dispone la propia Ley, el historial clínico laboral del trabajador, debiendo tenerse en cuenta que, en cuanto historia clínica, la misma se sometería a lo establecido en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que impone la llevanza de la misma a los centros sanitarios o profesionales que realicen las actuaciones sanitarias en relación con el paciente, en este caso el trabajador que se somete a las pruebas que implican la realización de acciones de vigilancia de la salud.

Además, deben establecerse procedimientos para garantizar los **derechos de acceso, rectificación y supresión de las personas trabajadoras**.

Cuando se trate del acceso a la historia clínica, debe recordarse que la legislación específica impone deberes como la **limitación del acceso a las anotaciones subjetivas** del facultativo, la existencia de límites a la rectificación contenidas en regulaciones sectoriales en materia de Seguridad Social, o la imposibilidad de

proceder a la **supresión** de los datos que deban conservarse en virtud de la normativa sanitaria. En todo caso, deberá contestarse la petición motivando la denegación.

En relación con la historia clínica, la exigencia de fijar **perfiles de usuario** puede derivar de la Ley 41/2002, de 14 de noviembre, que define de modo muy preciso el perfil funcional de cada tipo de persona trabajadora.

> «1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.
>
> 2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.
>
> (...)
>
> 4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.
>
> 5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.
>
> 6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto» (art. 16 de la Ley 41/2002, de 14 de noviembre).

www.aepd.es

@aepd_es