Universidad Zaragoza
1542

Trabajo Fin de Grado

La protección de datos personales en la relación laboral

Autor:

Carlos Sola Ros

Director:

Alba Pérez Polo

Facultad de Derecho; Universidad de Zaragoza

2021/2022

INDICE

Listado de abreviaturas 2

I. INTRODUCCIÓN 3

1. Cuestión tratada en el TFG 3
2. Razón de la elección del tema y justificación de su interés 4
3. Metodología seguida en el desarrollo del trabajo 5

II. PROTECCIÓN DE DATOS EN EL DESARROLLO DE LA RELACIÓN LABORAL 6

1. Protección de datos en los procesos de selección de trabajadores 7
2. Cesión de datos del trabajador a terceros 9
3. Protección de datos en las Relaciones Colectivas 11
4. Publicación de datos de productividad 13
5. Tratamiento de categorías especiales de datos personales 13
6. Canales internos de denuncias 18
7. La extinción de la relación laboral 20

III. DERECHOS DE LOS TRABAJADORES EN EL AMBITO DE PROTECCIÓN DE DATOS 22

1. Derecho de los trabajadores a recibir información complementaria 23
2. Derecho de Acceso 24
3. Derecho de Rectificación 24
4. Derecho de Supresión 25
5. Derecho de Limitación del tratamiento 26
6. Derecho de Portabilidad 26
7. Derecho de Oposición 27
8. Derecho a no ser objeto de decisiones automatizadas 27
9. Derecho a la tutela efectiva 27

IV. CONTROL DE LA ACTIVIDAD LABORAL 30

1. Control informático y de las comunicaciones 30
2. Control de la videovigilancia 31
3. Geolocalización 33
4. Registro de la jornada 33
5. Control de Acceso 34
6. Control de la falta de asistencia por enfermedad o accidente 34
7. Detectives Privados 35

V. CONCLUSIONES 36

VI. BIBLIOGRAFIA 37

VII. ANEXO 39

LISTADO DE ABREVIATURAS UTILIZADAS:

- **RGPD:** Reglamento General de Protección de Datos de la Unión Europea.
- **LOPD:** Ley Orgánica de Protección de Datos.
- **AEPD:** Agencia Española de Protección de Datos.
- **UE:** Unión Europea.
- **LRJS:** Ley Reguladora de la Jurisdicción social
- **LGT:** Ley General Tributaria.
- **LOLS:** Ley Orgánica de Libertad Sindical.
- **ETT:** Empresa de Trabajo Temporal.
- **LPRL:** Ley de Prevención de Riesgos Laborales.
- **LSS:** Ley General de la Seguridad Social.
- **TEDH:** Tribunal Europeo de Derechos Humanos.
- **LOITSS:** Ley Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social.
- **LSP:** Ley de Seguridad Privada.
- **CP:** Código Penal.
- **ET:** Estatuto de los Trabajadores.
- **TRLISOS:** Texto Refundido de la Ley sobre Infracciones y Sanciones del Orden Social.
- **STC:** Sentencia del Tribunal Constitucional.
- **TSJ:** Tribunal Superior de Justicia.
- **SAN:** Sentencia del Audiencia Nacional.
- **STS:** Sentencia del Tribunal Supremo.

I . INTRODUCCIÓN

1. Cuestión tratada en el TFG

La protección de datos personales es un tema que se encuentra en constante crecimiento de forma global desde principios del siglo XXI y que se enfrenta a nuevos retos y a la necesidad de nueva regulación de forma prácticamente paralela al desarrollo de nuevas tecnologías.

Aunque la búsqueda de una mayor protección en los datos personales es un aspecto que preocupa a prácticamente la totalidad de gobiernos del mundo, es cierto, que los países europeos, y más concretamente, los pertenecientes a la Unión Europea (en adelante, «UE») siempre han ido un paso por delante que la mayoría del resto de países. Como hemos mencionado, la UE ha ido siempre un paso por delante en la protección de este ámbito, pero en 2016 se produjo una verdadera revolución en la regulación de todos los diferentes ámbitos que engloban esta materia, a través del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, «RGPD»). Este reglamento se aplica plenamente (o de forma directa) desde el 2018.

Debido a la importancia del RGPD y para una mayor comprensión del trabajo se procede a explicar la estructuración del mismo. Con anterioridad al articulado, el Reglamento dispone de 173 Considerandos, entendiéndose cada uno de ellos como las razones o motivos que apoyan o sirven de fundamento al texto del RGPD. Posteriormente, el RGPD se encuentra comprendido por 99 artículos, divididos en 11 capítulos.

El RGPD se presenta como una norma de aplicación obligatoria para todos los países miembros de la Unión Europea, pero, además, puede ser complementada y reforzada por normativas nacionales. En el caso de España, la ley con la que se adapta al ordenamiento jurídico nacional el Reglamento Europeo y con la que se refuerzan ciertos aspectos es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, «LOPD»). Además, el RGPD establece la necesidad de nombrar una autoridad nacional de Protección de Datos, que en el caso español es la Agencia Española de Protección de Datos (en adelante, «AEPD»). La función principal de la AEPD es asegurar el cumplimiento de las legislaciones en Protección de Datos,

atendiendo a reclamaciones y peticiones de interesados, así como investigando por su parte posibles incumplimientos y ofreciendo información a los usuarios sobre cómo se deben de aplicar de forma correcta las leyes, a través, de Guías e Informes Jurídicos.

A raíz de la Sentencia del Tribunal Constitucional (en adelante, «STC») 39/2016, de 3 de marzo de 2016, se llega a la conclusión que los tratamientos de Datos Personales en el entorno laboral deben de cumplir tres características: (i) tratamiento justificado, (ii) tratamiento idóneo y (iii) tratamiento equilibrado.

Otro principio que debe resultar de aplicación es el principio de minimización que indica que únicamente se deben utilizar aquellos Datos Personales que resultan fundamentales para el tratamiento legitimado que pretende llevar a cabo la empresa. Las bases legitimadoras de los tratamientos vienen recogidas en el artículo 6 RGPD y, en el ámbito laboral, lo más frecuente es que el contrato actúe como base legitimadora para la mayoría de los tratamientos. Aunque también es habitual que se utilicen otras como el interés legítimo, el consentimiento del trabajador o las obligaciones legales (sobre todo en materia de Prevención de Riesgos Laborales).

2. Razón de la elección del tema y justificación de su interés

El tema resulta de gran interés y actualidad, al ser la protección de datos de carácter personal un campo en boga y con más importancia cada día. Prueba de este crecimiento son los siguientes datos que aporta la AEPD:

- En 2021 las denuncias a la AEPD crecieron un 35 % y las resoluciones en procedimiento sancionador un 49%.
- Se incrementaron las multas impuestas en resolución definitiva en 2021, cuyo importe medio se ha triplicado con respecto al año anterior, y cuyo importe global ha aumentado un 337%. Prueba del incremento de la intensidad en las sanciones son los algo más de 8 millones interpuestos a Vodafone o los 6 millones a los que tendrá que hacer frente La Caixa.
- Prueba de que este crecimiento va a continuar es que la AEPD tiene aprobado un incremento de plantilla para 2022 y 2023.

Atendiendo a estos datos, parece claro que el cumplimiento de la normativa relativa a la Protección de Datos es cada vez más importante para todas las empresas, ya sean más o menos grandes.

3. Metodología seguida en el desarrollo del trabajo

A lo largo de este trabajo se va a desarrollar la normativa en Protección de Datos Personales en el entorno laboral. Para ello hay que combinar la correcta aplicación de las legislaciones en protección de datos, RGPD y LOPD, con la legislación nacional en el ámbito laboral, es decir, el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (en adelante, «ET»). Además de estas normas, para actuar de forma más concreta y eficiente, el artículo 88 RGPD, titulado «Tratamiento en el ámbito laboral», establece que será posible la creación de disposiciones legislativas y/o de convenios colectivos, para establecer normas más específicas que garanticen una mayor protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral.

El trabajo se va a dividir en tres partes. En primer lugar, se estudiarán como influye la regulación actual sobre las relaciones laborales del día a día, posteriormente, se desarrollarán los derechos de los empleados en relación con la protección de datos y, por último, se explicarán los diferentes controles que puede ejercer la empresa sobre el trabajador, así como sus límites.

II. PROTECCIÓN DE DATOS EN EL DESARROLLO DE LA RELACIÓN LABORAL

La protección de datos en el desarrollo de la relación laboral parte del concepto general de dato personal que define el RGPD en su artículo 4.1 como: «toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número 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 de dicha persona. ».

Como se ha mencionado con anterioridad, el tratamiento de los datos personales en el ámbito laboral viene permitido, en la mayoría de las ocasiones, por el contrato de trabajo, que actúa como base legitimadora. Ahora bien, no la totalidad de los tratamientos se encuentra amparada por el contrato laboral, siendo necesaria en ciertos supuestos la licitud legal del tratamiento o el consentimiento del trabajador.

Atendiendo a estas posibles bases legitimadoras, la normativa de protección de datos personales debe aplicarse en el ámbito laboral incluso con anterioridad a que dé comienzo la relación laboral. Por tanto, resulta de aplicación la normativa desde el momento en el que comienza el proceso de selección, hasta que se extingue la relación laboral, pasando por la prestación del servicio.

También resulta interesante recordar que, en el ámbito laboral, el artículo 88 RGPD indica que: «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». De este precepto se extrae la posibilidad de que cada entidad negocie su propio convenio colectivo, con el objetivo de ajustarlo lo máximo posible a sus características y necesidades propias. Evidentemente, estos convenios se deben de ajustar al contenido mínimo exigido por el RGPD, por la LOPD y por las distintas guías y resoluciones que emite la AEPD, siendo este el contenido que se procede a detallar.

1. Protección de datos en los procesos de selección de trabajadores

La base legitimadora del tratamiento de datos en los casos de selección de trabajadores en virtud del artículo 6.1 b) RGPD que indica la licitud de los tratamientos cuando: «el interesado es parte o para la aplicación a petición de este de medidas precontractuales», pudiéndose entender como petición por parte de un trabajador el envío de un currículum o el acudir a un proceso de selección. En el mismo sentido, se establece en el Considerando 44 RGPD que la intención de concluir un contrato debe otorgar licitud al tratamiento.

1.1 Fase de recepción del currículum

La forma habitual de comenzar un proceso de contratación suele ser el envío del currículum por parte de la persona que pretende ser contratada. La AEPD establece tres formas posibles en las que se produce este hecho:

- Currículum es presentado de forma directa por el candidato. Hoy en día, un gran número de empresas ofrecen la posibilidad de poder presentar a través de la página web el currículum para el acceso a un puesto de trabajo. En caso de que la llegada de datos personales se produzca por esta vía, las empresas deben establecer un procedimiento de información al interesado de forma que confirme que conoce las condiciones del tratamiento. Lo mismo sería aplicable para casos en los que el interesado remita de forma autónoma el currículum por correo electrónico o postal.

  En el supuesto en el que se produzca la presentación del currículum en mostrador u oficina, se le deberá informar en el mismo instante de las características del tratamiento. Tanto en este supuesto como en el anterior lo más efectivo parece establecer como requisito para la entrega del currículum la aceptación del recibimiento de información.

- La compañía lanza una campaña o anuncio para la selección de personal. En este supuesto, la empresa debe incluir en la campaña la información que el artículo 13 RGPD establece. Entre la información a compartir destaca: la identidad y los datos de contacto del responsable y, en su caso, de su representante; los datos de contacto del delegado de protección de datos, en su caso; los fines del tratamiento

y la base jurídica del tratamiento; el plazo de conservación de los datos personales; los derechos del interesado; y, su posibilidad de reclamación ante la AEPD.

- Una empresa privada de colocación remite el currículum a otra compañía. En este caso la empresa de colocación debe solicitar el consentimiento de los candidatos para proceder a la cesión de sus datos a otra empresa con el fin de que se produzca la contratación.

1.2 Desarrollo del proceso de selección

Los procesos de selección se realizan de forma habitual a través de entrevistas al interesado por parte de una persona de la compañía. Las preguntas deben dirigirse con exclusividad a valorar las competencias y capacidades del interesado para el puesto que oferta la compañía. Cabe destacar que los datos que se recaban o se deducen a partir de las preguntas que se realizan no podrán ser objeto de tratamiento, debido a que la mera contestación no se considera base legitimadora suficiente. En el caso de que las entrevistas vayan más allá de simples preguntas y, por ejemplo, se realice una prueba, esta deberá ser acompañada por la información de datos personales pertinente, indicando que la única finalidad del tratamiento será el proceso de selección.

Una actuación frecuente en los procesos de selección es la solicitud de información y referencias a antiguas empresas del candidato, si bien, esta práctica únicamente será lícita cuando los datos de la otra empresa sean otorgados por el candidato.

En los casos en los que los datos personales recopilados supongan una discriminación de cualquier tipo (sexo, edad, raza, religión, afiliación sindical…) a la hora de acceder al puesto de trabajo, se incurre en una infracción muy grave regulada en el artículo 16.1 c) 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 del Orden Social (en adelante, «TRLISOS»).

Como establece el artículo 40.1 c) TRLISOS estas infracciones se sancionan: «en su grado mínimo, de 7.501 a 30.000 euros; en su grado medio de 30.001 a 120.005 euros; y en su grado máximo de 120.006 euros a 225.018 euros. ». Ahora bien, en determinados sectores (como los relacionados con el Blanqueo de Capitales o con el cuidado de menores), sus propias normas de regulación permiten el tratamiento y solicitud de ciertos datos especiales como podrían ser los relativos a infracciones administrativas y penales.

1.3 Finalización del proceso de selección

Una vez finalizado el proceso de selección, con carácter general, los datos deberían ser destruidos tal y como se debe indicar en la información dada al interesado, ahora bien, pueden existir un par de excepciones. En el caso de que una compañía quiera mantener los datos obtenidos para ser usados en futuros procesos de selección o para remitirlos a otras empresas del grupo, se debe solicitar consentimiento al candidato para este tratamiento concreto, tal y como establece el artículo 29 del Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de trabajo sobre protección de datos.

Otra excepción resulta del caso en el que la empresa decida finalmente proceder a la contratación del candidato, en cuyo caso está permitido el mantenimiento de los datos con el objeto de incentivar el dinamismo y eficiencia del proceso al evitar solicitar los mismos datos en dos momentos diferentes.

2. Cesión de datos del trabajador a terceros

Con carácter general, para que se pueda producir la cesión de datos de un trabajador por parte del empresario a un tercero es necesario que medie consentimiento del empleado. En caso contrario se podría incurrir en una vulneración de los derechos fundamentales del trabajador. Sin embargo, como se procede a analizar a continuación, existen una serie de supuestos en que la cesión de datos del trabajador no está sujeta a su consentimiento, estando amparada por una obligación legal o un interés legítimo del empleador.

Cabe indicar que en los casos en los que se contrate con otra empresa para llevar a cabo uno de los tratamientos que se proceden establecer, es obligación del Responsable el comprobar que la empresa a la que se le van a ceder los datos cumple con los requisitos mínimos en materia GDPR.

2.1 Cesión de datos del trabajador permitida por una obligación legal

La empresa Responsable de los datos tendrá la obligación legal de proceder a la cesión de ciertos datos de los trabajadores. Se podrá proceder esta cesión en determinados supuestos, atendiendo a la legislación sectorial y el RGPD:

- Cesión de datos a los representantes de los trabadores y sindicales (Se analizará en profundidad en el siguiente punto). Tal y como establecen los artículos 64 ET y 10 de la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical (en adelante, «LOLS»), en relación con el 6.1 RGPD.

- Cesión de datos a la Agencia Tributaria. A tenor del artículo 93.1 de la Ley 58/2003, de 17 de diciembre Ley General Tributaria (en adelante, «LGT»).
- Cesión de datos a otras entidades públicas como pueden ser la Tesorería General de la Seguridad social, la Mutua de accidentes de Trabajo y enfermedad Profesional o las encargadas de las inspecciones de trabajo.
- Cesión de datos a entidades con la que se contrata el tratamiento de pensiones o seguros de vida. El Real Decreto legislativo 1/2002, de 29 de noviembre por el que se aprueba el texto refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, establece que los compromisos adquiridos por la empresa en este ámbito se deberán instrumentar desde que comience el devengo de su coste. Por lo que esta obligación permite a las compañías ceder los datos de los trabajadores a la empresa con la que contrate.

2.2 Subcontratación de empresas

El artículo 42 ET ampara la subcontratación de obras y servicios. Para estos supuestos no será pertinente el consentimiento del empleado, ya que el tratamiento viene amparado por el contrato de trabajo firmado. Sin embargo, sí que será necesario, de acuerdo con el artículo 42.3 ET en relación con el 13 GDPR, informar al trabajador de que se va a producir la cesión de sus datos con la finalidad que proceda. También se deberá informar a los representantes de los trabajadores de los datos básicos de la subcontratación, que deberán comprender: (i) Nombre y demás datos de la empresa subcontratista, (ii) objeto y duración, (iii) lugar de ejecución, (iv) número de personas y, (v) medidas previstas para la coordinación. En estos supuestos, la empresa a la que se ceden los datos se convertirá en Responsable del tratamiento, por lo que la empresa cedente de los datos debe asegurarse de que cumple todas las responsabilidades que establece el artículo 24 RGPD.

De acuerdo con el Informe Jurídico 0412/2009 de la AEPD, únicamente se podrán ceder los datos de los trabajadores subcontratados y solo aquellos datos necesarios para la prestación de la obra o servicio subcontratado.

La AEPD establece que la legitimación dada por este artículo también es aplicable a los supuestos de subcontratación de la confección de nóminas, los boletines de cotización y otros servicios análogos. Estos documentos son susceptibles de contener ciertos datos categorizados como «especiales», cuyo tratamiento viene legitimado por el art. 9.2.b) en relación con el art. 6.1.c) del RGPD.

2.3 Cesión de datos a empresas del Grupo

Dentro de un grupo de empresas, cada una de ellas cuenta con personalidad jurídica propia y debe ser considerada como Responsable del tratamiento de sus trabajadores. El Considerando número 48 RGPD señala que: *«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»*. A pesar de lo establecido en este Considerando, la AEPD matiza que, para poder centralizar la información de todos los trabajadores de un grupo en un único fichero, será necesario que se celebre un contrato en la empresa donde vayan a residir los datos quede como encargada del tratamiento[1].

3. Protección de datos en las Relaciones Colectivas

El artículo 64 ET regula la obligación legal de las empresas de comunicar los datos de los trabajadores a los Representantes de los Trabajadores, mientras que el artículo 10 LOLS hace lo propio con los Representantes Sindicales. El objetivo único de esta transmisión de datos es poder proceder al derecho de defensa que tienen los trabajadores, por lo que los datos no podrán ser utilizados para otras finalidades.

3.1 Datos transmitibles

Del artículo 64 ET se puede extraer que es obligatorio informar a los Representantes acerca de, entre otras:

- Situación económica y contable de la compañía.
- Evolución probable del empleo.
- Inicio y fin de la relación laboral.
- Modificaciones de la relación laboral.
- Copia básica del contrato de trabajo.
- Sanciones por faltas muy graves.
- Absentismo laboral.

[1] El RGPD define en el artículo 4.7 al Encargado del Tratamiento como: «la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. ».

Además de los datos que obliga la ley a traspasar, se puede establecer el traspaso de datos adicionales por convenio tal y como establece el artículo 64.9 ET. Todas estas cuestiones suponen el traspaso de una gran cantidad de datos de carácter personal, ya que muchas de estas situaciones conllevan el traspaso de datos identificativos. En esta situación debe primar el principio de minimización de datos personales, por el que únicamente se deben de traspasar los datos esenciales para poder ejercer de forma correcta la defensa de los trabajadores.

En este sentido se pronuncia la Sentencia del Tribunal Supremo (en adelante, «STS») 572/2018 de 7 de febrero, de la Sala de lo Social que señala la no admisibilidad del traspaso y posterior tratamiento de datos personales privados de los trabajadores, pero sí de datos que permitan la defensa de los trabajadores como la identificación de las personas que ocupan un determinado puesto de trabajo o el correo electrónico corporativo. De igual forma se pronuncia el Auto del TC 29/2008, de 28 enero también hace hincapié en este aspecto, señalando la prohibición de compartir datos privados de los trabajadores como pueden ser el DNI o domicilio.

En cuanto a aspectos más difusos como puede ser el salario, la STS de 19 de febrero de 2009, Sala de lo Social señala que es correcto compartir la información de los salarios, pero categorizada en departamentos o secciones, no siendo conforme a la legalidad el traslado de los salarios individuales de cada trabajador. Se aprovecha para señalar que el artículo 28.2 ET establece la obligación legal para el empleador de llevar a cabo un registro de salarios, en los que deben aparecer los valores medios desagregados por sexo y grupos profesionales.

3.2 Cuota sindical

Resulta importante tener en cuenta que la afiliación sindical de los trabajadores conlleva un descuento de esta cuota sindical en el salario del trabajador. A pesar de que el artículo 9.1 RGPD prohíbe el tratamiento de datos personales relacionados con la afiliación sindical, el preámbulo de la LOPD indica que sí es lícita la comunicación con la finalidad de descuento de la cuota sindical. Es imprescindible que medie el consentimiento del trabajador (artículo 11.2 LOLS) para que se pueda producir la comunicación de la afiliación por parte del sindicato a la compañía. La AEPD establece en sus Informes Jurídicos 0231/2008 y 0033/2010, que para cumplimentar el consentimiento basta con

que el trabajador complete una ficha en el momento de la afiliación, en la que autorice de forma específica este tratamiento.

3.3 Tablón de anuncios

Como último punto de este apartado, resulta necesario conocer las peculiaridades acerca del tablón de anuncios obligatorio que deben tener las empresas, tal y como indican los artículos 81 ET y 8.2 LOLS. Se establece que el tablón debe situarse en un lugar en el que únicamente pueda ser consultado por los afectados de la noticia y no por todos los trabajadores de la compañía. Además, el responsable de este tablón será el sindicato y no el empresario.

La evolución de las nuevas tecnologías ha llevado a que muchas empresas pongan a disposición este tablón de anuncios a través de Internet. La Sentencia de la Sala de lo Contencioso de la Audiencia Nacional 3578/2009, de 8 de junio, señala que en estos casos es imprescindible que se sitúe en la Intranet de la empresa, siendo necesario disponer de usuario y contraseña para poder acceder.

4. Publicación de datos de productividad

Resulta clave para conocer la licitud de los datos de productividad el realizar una adecuada ponderación entre el interés legítimo existente y la lesión de derechos del trabajador. Resultará pertinente la publicación de los datos de productividad en aquellos supuestos que sean absolutamente necesarios como puede ser el abono de un complemento salarial a los trabajadores que consiguen una mayor productividad, encontrando el tratamiento amparo en el interés legítimo del empleador regulado en el artículo 6.1 f).

De todas maneras, cuando se realice la publicación de estos datos se debe realizar de forma discreta, de forma que no puedan acceder trabajadores externos a la empresa y sin usar datos directos vinculados al empleado, por lo que habrá que establecer un código interno que únicamente conozcan el empleador y el empleado. Así lo indica la AEPD en su informe 183-2018, que, además, señala la prohibición de uso de estos datos para tratamientos futuros.

5. Tratamiento de categorías especiales de datos personales

El artículo 9.1 RGPD señala como categorías especiales de datos personales*:* «que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o

filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. ». En el apartado anterior ya se ha explicado como de deben tratar los datos relativos a la afiliación sindical y en este apartado se indagará más en la forma de tratamiento que deben de seguir muchos de los demás datos especiales.

Para poder proceder al tratamiento de estas categorías de datos será necesario que concurra una de las circunstancias que señala el apartado 2 del artículo 9 RGPD, es decir:

- El interesado dio su consentimiento explícito para el tratamiento.
- 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.
- El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.
- El tratamiento es efectuado por un 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 y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.
- El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.
- El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.
- El tratamiento es necesario por razones de un interés público esencial.
- El tratamiento es necesario para fines de medicina preventiva o laboral.
- El tratamiento es necesario por razones de interés público en el ámbito de la salud pública.
- El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

5.1 La protección de datos de salud

En el caso de los datos de salud, la base legitimadora para su tratamiento es una combinación del contrato de trabajo junto al establecimiento de medidas legales en el ET y en la Ley de Prevención de Riesgos Laborales (en adelante «LPRL»).

El Responsable del tratamiento dependerá de la forma en la que se realice el tratamiento, en caso de que la empresa tenga un servicio propio, la propia empresa actuará como Responsable. Por otro lado, en el caso de que se proporcione un servicio externo, la empresa actuará como Encargada del tratamiento. En el caso de cambiar la compañía que ofrece el servicio externo, la portabilidad de los datos está permitida por la legislación.

El artículo 22.1 LPRL nos indica que es una obligación para el empresario proporcionar un servicio que garantice la vigilancia periódica a sus trabajadores, pero que para poder proceder a la recogida de los datos y posterior tratamiento de los datos resulta imprescindible el consentimiento del trabajador, bastando con un único consentimiento para los dos supuestos. Sin embargo, el mismo precepto, señala que, previo informe de los Representantes de los trabajadores habrá tres supuestos en los que será obligatoria la vigilancia de la salud:

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.

El mismo artículo 22 LPRL señala que únicamente deberán tener acceso a los datos personales obtenidos el propio trabajador, el personal médico (que tienen un deber de confidencialidad) y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que el empresario tenga acceso a ellos, más allá de conocer la aptitud del trabajador. Resulta obligatorio además que, sea o no obligatoria la recogida y tratamiento, el empresario cumpla con su deber de información al trabajador. Además, la AEPD indica que la cesión de los datos no será permisible, ni con el consentimiento del trabajador dado, al no resultar este completamente libre.

El Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley General de Seguridad Social (en adelante «LSS») regula los datos personales que son de utilización cuando se da un caso de Incapacidad Temporal. En estos supuestos, existe la opción de que las Mutuas de Accidentes de trabajo o Enfermedades Profesionales lleven a cabo la gestión de las bajas por Incapacidad Temporal, actuando como Responsables del tratamiento. Esto conlleva el traspaso de una gran cantidad de datos, para los que no es necesario el consentimiento del trabajador dado que se considera una obligación legal. Ahora bien, estos datos deberán ser tratados con la finalidad única de recuperación y protección del trabajador, no pudiendo ser comunicados al empresario o empresa, con la excepción única de que sea necesaria la investigación del accidente o enfermedad.

5.2 Datos Personales ante situaciones de acoso en el entorno laboral

La AEPD ha establecido una serie de requerimientos relativos a los datos a tratar y la forma de tratar los mismos en estas situaciones:

1. Los procedimientos sancionadores y tratamiento de datos en la empresa frente al acosador no requieren del consentimiento de la persona acosada.
2. Únicamente se podrá solicitar a la persona acosada información pertinente para el esclarecimiento de los hechos, sin poder usar sus datos personales obtenidos en el curso de la investigación o con anterioridad con la empresa para otra finalidad distinta a la del procedimiento sancionador, debiendo garantizar en todo momento su confidencialidad.
3. Deberá asignarse un código identificativo tanto a la persona supuestamente acosada como a la supuestamente acosadora, para una mayor protección de confidencialidad, sin que debe constar su identidad en ningún documento que no tenga como fin la sanción del acosador.
4. Una vez concluido el procedimiento sancionador, los datos deben ser bloqueados durante el período de prescripción de la sanción.
5. Los representantes de los trabajadores solo podrán conocer la identidad de la víctima en el supuesto de que sea imprescindible para el ejercicio de sus labores de representación.

6. Se debe informar, tanto a la persona acosada como a la supuestamente acosadora sobre el tratamiento de datos y sobre el ejercicio de los derechos de acceso, rectificación, oposición y supresión.

7. Se considerarán datos de categoría especial los datos médicos obtenidos durante la asistencia sanitaria que se haya proporcionado en casos de acoso, si esta es necesaria.

8. Para poder proceder a la cesión de los datos de la víctima será necesario su consentimiento, salvo determinados supuestos establecidos en la ley como puede ser la solicitud por parte de un juez.

5.3 Datos biométricos

El RGPD en su artículo 4.14 define los datos biométricos como: «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 se ha mencionado el artículo 9.1 RGPD establece los datos biométricos como una categoría especial de datos temporales, pero hay que aclarar que solo constituirán datos especiales cuando efectivamente consigan distinguir de manera inequívoca a una individuo.

La AEPD establece la necesidad de almacenar los datos biométricos en plantillas biométricas que se deberán de guardar, con carácter preferente, en un dispositivo personal. Será necesaria, además, una clave de encriptado especial para cada uno de estos dispositivos, como método de protección ante posibles accesos no deseados o autorizados, que pudiesen provocar una lectura, copia, modificación o supresión de estos datos. También se establece la necesidad de supresión de los datos biométricos una vez finalizado el motivo de su tratamiento, recomendado tener un sistema de supresión automática.

En los supuestos en los que se opte por un sistema de identificación biométrica (como se pueden considerar las fotografías que se anexan a tarjetas de identificación) será necesaria

llevar a cabo una Evaluación de Impacto[2], para poder conocer los riesgos y si resulta posible y licito llevar a cabo dicho tratamiento.

D) Datos genéticos

El artículo 4.13 define los datos genéticos como: «datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona».

Los datos genéticos llevan mucho tiempo siendo objeto de estudio. En 1989 el Parlamento Europeo emitió una Resolución sobre los problemas éticos y jurídicos de la manipulación genética, en la que comentaba que los análisis genéticos en las empresas debían ser prohibidos. Hoy en día, con el RGPD, se admite el tratamiento de datos genéticos con consentimiento del trabajador, pero únicamente cuando sea necesario en la esfera de la prevención de riesgos laborales. Fuera de este ámbito se entiende que el consentimiento podría estar viciado por querer mantener o asegurar el puesto de trabajo.

Siguiendo la normativa de riesgos laborales, si podrá llevarse a cabo la obtención y posterior tratamiento de datos genéticos en los supuestos en los que, por desarrollar una labor de alto riesgo, puedan ser de utilidad para medir posibles efectos nocivos sobre la salud del trabajador. En estos supuestos también será imprescindible que medie el consentimiento del trabajador. La existencia de riesgos para la salud del trabajador debe quedar acreditada.

6. Canales internos de denuncias

El artículo 24 LOPD permite la creación de estos canales internos de denuncias, también conocidos como «*whistleblowing*». En todo caso, se determina en el punto primero de este precepto que se creación será «lícita», por lo que se puede extraer que no será de creación obligatoria para las compañías.

El objetivo de estos canales es crear un medio seguro en el que los trabajadores puedan denunciar de forma segura determinadas conductas o actuaciones, llevadas a cabo por

[2] La AEPD define la Evaluación de Impacto como «una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. ».

auditores u otros trabajadores, contrarias a la legalidad o a la normativa interna de la empresa.

Hoy en día, con carácter general, estos buzones se establecen vía *online*, aunque también se podrán situar en las oficinas o por vía telefónica. Puede ser gestionado de dos formas diferentes:

- Por un departamento propio de la empresa: en este caso, se recomienda que el departamento se dedique con exclusividad a esta función, para no poder ser influido por otros departamentos.
- Por una compañía externa: en el supuesto de que una compañía externa se encargue del estudio de los hechos, será necesaria la transmisión de una serie de datos personales. Para lo cual, se deberá informar tanto al denunciante como al denunciado.

La AEPD establece en el Informe Jurídico 128/2007 siete mínimos sobre el tratamiento que se debe dar a los datos personales en estos supuestos:

1. Será necesario el consentimiento del trabajador para el tratamiento de los datos personales siempre y cuando la denuncia vaya más allá de la relación laboral. Si se entiende dentro de la relación laboral, se entenderá como un desarrollo del contrato laboral, sin ser necesario el consentimiento.

2. En caso de disponer de estos buzones, la empresa deberá comunicar, de forma obligatoria, a sus trabajadores su existencia, finalidad, forma de uso y funcionamiento dentro de la compañía.

3. Únicamente podrán tener acceso a los datos personales las personas que desarrollen la investigación de los hechos y los Responsables del sistema.

4. Se debe seguir el principio de minimización, incorporándose al sistema los datos imprescindibles del denunciante, denunciado, los hechos y el resultado tras las investigaciones.

5. A la mayor brevedad se deberá comunicar al denunciado la existencia de dicha denuncia, sin que se pueda revelar la identidad del denunciante.

6. Dentro de la información remitida a ambas partes, se debe establecer la posibilidad de ejercer los derechos de acceso, rectificación, oposición y supresión

7. La empresa debe suprimir los datos en un máximo de tres meses si los hechos no se hubiesen comprobados y hubiese finalizado la investigación. En caso contrario se deberán conservar hasta la celebración del juicio, al poder utilizarse como medio de prueba.

7. La extinción de la relación laboral

La extinción de la relación laboral trae consigo el tratamiento de una cantidad importante de datos personales, que encuentran su licitud en la obligatoriedad de extinguir la relación laboral de la forma adecuada.

La comunicación del despedido al trabajador se realiza de manera oficial a través de una carta de despido. En ella, se contienen datos personales del trabajador e incluso pude contener datos de clientes siempre que sea «pertinente y adecuado» establece la AEPD. En esta carta de despido se debe incluir el motivo del despido, aunque se debe prestar especial diligencia a que no aparezcan datos que el empleador no pueda conocer, singularmente cuando se trate de datos de categorías especiales, en este sentido se pronuncia la STS 5138/2005, de 22 de julio, Sala de lo Social. Además, las compañías y los empresarios deben establecer las medidas de seguridad que consideren oportunas para que la carta de despido (y los datos personales que contiene) lleguen al empleado afectado y no a un tercero, supuesto en el que incurriría en una infracción administrativa.

Por otro lado, como se ha mencionado con anterioridad en este trabajo, la extinción de la relación laboral debería conllevar el bloqueo y supresión de los datos del trabajador afectado. Se le reconoce el derecho de interponer este derecho de supresión al trabajador, pero incluso se establece que debería de ser la propia empresa quien ejecutara este bloqueo, sin necesidad de intervención por parte del trabajador.

Ahora bien, las legislaciones sectoriales como la TRLISOS o la LGT establecen distintos periodos de tiempo durante los cuales se deben de conservar una serie de documentos una vez finalizada la relación laboral. En la mayoría de los casos, estos documentos contendrán datos personales, por lo que no será posible llevar a cabo una supresión total de los datos del trabajador hasta que no pasen los distintos periodos de prescripción establecidos en estas leyes.

En este sentido, el periodo más alto de conservación es establecido por la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (en adelante, «CP») en una de sus

modificaciones. Establece la prescripción de delitos relacionados con materias fiscales y laborales en 10 años, por lo que existe la posibilidad de que documentos relacionados con la actividad realizada por un trabajador sean solicitados, y por tanto deberán conservarse, durante este periodo de tiempo. Es decir, no es posible llevar a cabo una supresión total de los datos hasta pasados diez años desde la finalización de la relación laboral.

Para finalizar este apartado resulta interesante añadir dos supuestos. En primer lugar, el trabajador tendrá el derecho de acceder los datos personales que se encuentre en aquellos lugares que el trabajador ha estado utilizando en el ejercicio de sus actividades laborales. En segundo lugar, y siendo habitual en extinciones de la relación laboral amistosas, el empresario puede solicitar el consentimiento del trabajador para contactar con él en un futuro.

III. DERECHOS DE LOS TRABAJADORES EN EL AMBITO DE PROTECCIÓN DE DATOS

Con anterioridad al nuevo reglamento, los derechos relacionados con la protección de datos reconocidos a los trabajadores eran los derechos de acceso, rectificación y cancelación (este último, ha sido sustituido por el derecho de supresión). El RGPD ha añadido una mayor protección, poniendo a disposición del trabajador una gama más amplia de derechos. Cabe remarcar que los derechos reconocidos en este ámbito son limitados, es decir, pueden verse restringidos en el caso de que intervengan otros intereses de mayor entidad.

Antes de conocer todos los derechos existentes para los trabajadores, cabe indicar que la Autoridad de Control de cada país tiene la capacidad de determinar las multas administrativas que correspondan cuando se incumplan alguno de los derechos de protección de datos. Por ende, en el caso de estudio, la AEPD tendrá la capacidad de sancionar a los Responsables del tratamiento[3] cuando incumpla alguno de los derechos, en materia laboral, que se van a mencionar a continuación. Como establece el artículo 83.1 RGPD las sanciones que se impongan deben ser efectivas, proporcionadas y disuasorias. Además, como se indica en el segundo punto del mismo artículo, las sanciones deben ser graduadas atendiendo, entre otras cosas, a su: naturaleza, gravedad, duración, número de afectados, intencionalidad y reincidencia. En los apartados 4, 5 y 6 del precepto mencionado se establecen dos límites máximos para las sanciones:

- 10 millones de euros o un 2 % del volumen de negocio total anual global del ejercicio financiero anterior, en los siguientes supuestos: No aplica en el ámbito laboral.

- 20 millones de euros o un 4 % del volumen de negocio total anual global del ejercicio financiero anterior: Se trata del límite aplicable al ámbito laboral y por tanto el que se establecerá para el incumplimiento de los derechos que se van a explicar en el presente apartado.

Hay que reseñar la obligación del Responsable del tratamiento de facilitar el ejercicio de los derechos mencionados a los trabajadores, para lo que es necesario informar sobre los

[3] El RGPD define en el artículo 4.7 al Responsable del Tratamiento como: «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. ».

derechos existentes y su forma de ejercicio, por lo que se va a comenzar este apartado hablando del deber complementario de información por parte de la empresa y el derecho del trabajador de recibirlo.

1. Derecho de los trabajadores a recibir información complementaria.

Nace del Considerando número 60 del RGPD en el que se señala que: «El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. ». El mismo precepto indica que se debe proceder a la entrega de esta información complementaria, aun cuando los datos personales se obtengan de forma directa del interesado.

El momento de recibir la información varía en función de si los datos son aportados por el trabajador o no. Por un lado, en el caso de ser aportados por el trabajador, a tenor del artículo 13.2 RGPD, el responsable del tratamiento deberá facilitar esta información en el mismo momento en el que se obtengan los datos personales. Por otro lado, el artículo 14.2 RGPD señala que, si los datos no son aportados por el trabajador se deberá suministrar en un plazo razonable o si es necesario comunicarse con el trabajador se le deberá informar en la comunicación.

El modo de presentar la información por parte de la empresa es siguiendo el modelo de capas o niveles, de acuerdo con la *Guía para el cumplimiento del deber de informar* que proporciona la AEPD. Este modelo consiste en aportar en el momento y medio por el que se recojan los datos un primer bloque de información básica o resumida. La información que se debe aportar en este primer momento es:

- Los datos del responsable del tratamiento y del DPD.
- Las finalidades del tratamiento y su base jurídica.
- Los destinatarios de los datos personales.

En un segundo momento posterior, se debe remitir el resto de información de una forma más detallada y concreta y en un medio más adecuado, creando la segunda capa que debe recibir el nombre de «Información sobre el tratamiento de datos personales de empleados», de acuerdo con el Informe Jurídico 0325/2009 de la AEPD. Además de la

información anterior, explicada más exhaustivamente, se debe presentar la siguiente información:

- El plazo de conservación de los datos.
- Los derechos de los trabajadores relativos a sus datos personales.
- Las categorías de los datos.
- La posibilidad de presentar reclamación ante la AEPD.
- Posibles finalidades futuras del tratamiento.

2. Derecho de Acceso

A raíz del artículo 15 RGPD se puede extraer que, el derecho de acceso en el ámbito laboral reconoce el derecho de los trabajadores a obtener una confirmación por parte del responsable del tratamiento acerca de si se están tratando o no sus datos personales. Además, en el caso de que se estén tratando, el trabajador tiene derecho a recibir información acerca de:

- Los fines del tratamiento.
- Las categorías de datos personales de que se traten.
- Los destinatarios a los que se comunicaron o serán comunicados los datos.
- Plazo previsto de conservación de los datos personales.
- La posibilidad de solicitud de otros derechos.
- El derecho a presentar una reclamación ante la AEPD.
- Cualquier información disponible sobre su origen, cuando los datos no se hayan obtenido del interesado.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles.

No se señala en ningún texto legislativo la forma exacta de presentar la información al trabajador, aunque sí se indica en la RGPD que en el caso de que el trabajador presente la solicitud por medios electrónicos y siempre y cuando no solicite lo contrario, la información deberá remitirse por los mismos medios. Por lo que se parece dar a entender que, con carácter general, este debe ser el principal modo de envío de los datos, siendo el más adecuado además desde un punto de vista ecológico y tecnológico.

3. Derecho de Rectificación

El artículo 16 del RGPD regula el derecho de rectificación, es decir, el derecho de los trabajadores a que se modifique sus datos personales cuando sean inexactos o a

completaros cuando sean incompletos. Para poder ejercer este derecho de forma efectiva, la LOPD exige que el interesado debe indicar en su solicitud de ejercicio de derecho cuales son los datos que desea modificar o completar, además de acompañarla de documentación que verifique la necesidad de la rectificación.

En el ámbito laboral, este derecho puede entrar en conflicto con la obligación del trabajador de informar de sus datos personales y los cambios que se produzcan en ellos que interponen una gran cantidad de empresas. Esto ocurre con aquellos datos que resultan necesarios y precisos para el desarrollo de la actividad laboral.

4. Derecho de Supresión

El interesado puede solicitar el borrado total de sus datos en las bases de datos del responsable del tratamiento siempre y cuando concurra una de las circunstancias establecidas en el artículo 17 GDPR. En el caso de una relación laboral se precisan cinco supuestos bajo los cuales el trabajador podría solicitar la supresión de sus datos personales:

- Cuando los datos personales no estén siendo utilizados para el fin original del tratamiento.
- Cuando sea preciso el consentimiento para su tratamiento y este decida retirarse.
- Cuando el tratamiento de datos sea ilícito. La finalización del contrato de trabajo y por ende de la relación laboral hace posible ejercer este derecho, incluso se debería de producir la supresión de forma directa por la empresa ya que el tratamiento deja de estar amparado por la relación laboral y pasa a ser, por tanto, ilícito.
- Cuando el tratamiento de los datos no se esté produciendo con la finalidad de cumplir y ejecutar el contrato de trabajo.
- Con motivo de que los datos deban ser suprimidos como son consecuencia de una obligación legal.

El responsable del tratamiento puede oponerse al derecho de oposición solicitado siempre y cuando concurra una de las siguientes cinco circunstancias:

- El tratamiento sea imprescindible para poder ejercer de forma correcta la libertad de expresión e información.

- El tratamiento sea necesario para el cumplimiento de una obligación legal como puede ser la necesidad de chequeos médicos para el desarrollo de la actividad laboral
- Se den motivos de interés público en el ámbito de la salud pública.
- Cuando existan motivos investigatorios, estadístico o de archivo en interés público.
- Cuando el mantenimiento de los datos sea necesario para la formulación, ejercicio o defensa de reclamaciones.

5. Derecho de Limitación del tratamiento

El artículo 18 RGPD regula la posibilidad que tienen los interesados de poner límite al tratamiento de sus datos personales. Se trata de una medida de menor entidad que el derecho de supresión ya que no supone el borrado de los datos. Un trabajador puede ejercer el derecho de limitación en cuatro circunstancias:

- Durante el plazo de verificación por parte del empleador cuando el trabajador reclama la inexactitud de sus datos personales.
- Ilicitud por parte del empleador del tratamiento, en el caso de que el empleado solicite la limitación y no la supresión de los datos.
- La persona trabajadora desea que la empresa mantenga los datos para determinados fines marcados pero que no sean utilizados para determinados tratamientos, cuando no son necesarios.
- Cuando el trabajador se haya opuesto al tratamiento de sus datos, tendrá derecho a la limitación durante el tiempo en el que se comprueban si el responsable del tratamiento tiene motivos legítimos.

6. Derecho de Portabilidad

Los interesados, tal y como señala el Considerando número 68 RGPD, tendrán derecho a la trasmisión de sus datos a otro responsable del tratamiento únicamente cuando la base para el tratamiento haya sido el consentimiento o la ejecución de un contrato. Es por ello que los trabajadores tendrán derecho a la portabilidad de sus datos, en prácticamente la totalidad de ocasiones, al basarse el tratamiento de sus datos en un contrato de trabajo.

Este derecho aparece regulado en el artículo 20 RGPD y consiste en el derecho de los trabajadores a recibir, en formato estructurado, los datos personales propios que le

incumban y que haya facilitado al Responsable. Además, podrá solicitar que se le den traslado a otro Responsable siempre y cuando esto sea posible. El deber de la empresa de mantener los datos para que el trabajador pueda ejercer este derecho finalizará en un plazo adecuado desde la finalización del contrato laboral para poder proceder al borrado de datos pertinente.

Cabe remarcar que el derecho de portabilidad no es exclusivo del momento en el que se produce la extinción del contrato de trabajo. Se podrá solicitar este derecho en el trascurso de la relación laboral, por ejemplo, por necesidades en servicios de pago.

7. Derecho de Oposición

Aparece regulado en el artículo 21 RGPD y en el ámbito laboral tiene ligeras implicaciones. Su aplicación principal es que en el caso de que el tratamiento tenga como base legitimadora la satisfacción del interés legítimo de la empresa o de un tercero, el trabajador tendrá el derecho de ejercer este derecho de oposición. Se le deberá conceder este derecho salvo que la compañía demuestre que sus motivos legítimos prevalecen sobre los del trabajador.

8. Derecho a no ser objeto de decisiones individuales automatizadas

Dentro de las decisiones automatizadas se encuentran incluidas la elaboración de perfiles, que resulta la decisión automatizada principal en las relaciones laborales. Podrá por tanto el trabajador ejercer este derecho cuando se elaboren perfiles con sus datos personales, entendiéndose como tal, toda forma de tratamiento de sus datos que evalúe aspectos personales, resaltando en el caso de las relaciones laborales la elaboración de perfiles vinculada al análisis del rendimiento en el trabajo. Este derecho se encuentra regulado en el artículo 22 RGPD, donde se señala que no será aplicable cuando la decisión automatizada tenga como base el consentimiento explícito del trabajador, esté autorizada por ley o sea imprescindible para la correcta ejecución del contrato.

9. Derecho a la tutela efectiva

El derecho a la tutela efectiva implica el reconocimiento por parte de la RGPD y la LOPD de acudir a la autoridad competente en materia de protección de datos o a los tribunales, en el supuesto de que el interesado considere que sus datos han sufrido vulneraciones en el curso de su tratamiento. Se subdivide por tanto en dos:

9.1 Derecho a la tutela efectiva ante la AEPD

Derecho del interesado (en este caso el trabajador) de acudir a la autoridad competente en materia de protección de datos, en el caso de España a la AEPD. Aparece regulado en el artículo 77 RGPD y en los 63 y ss. LOPD. La AEPD tiene un plazo de 3 meses para admitir o inadmitir las reclamaciones presentadas y, posteriormente, un plazo de 9 meses para resolverla.

9.2 Derecho a la tutela judicial efectiva

El titular de este derecho podrá ejercerlo como recurso a una resolución de la AEPD, o inclusive, podrá proceder a la interposición de la acción judicial sin ser requisito haber realizado una reclamación previa ante la agencia.

Más concretamente, en el ámbito laboral se disponen de dos procedimientos adicionales para que el trabajador pueda hacer valer este derecho:

- Proceso de tutela de derechos fundamentales: Se encuentra regulado en los artículos 177 a 184 de la Ley Reguladora de la Jurisdicción social (en adelante, «LRJS»). En el supuesto que nos ocupa, será el trabajador el que debe aportar pruebas suficientes acerca de la vulneración de sus derechos fundamentales en relación con sus datos personales. La sentencia, de 7 de marzo de 1995, del TSJ de Canarias señala que «el Ministerio Fiscal defenderá los derechos fundamentales y las libertades públicas, velando especialmente por la reparación de las víctimas», por lo que en el ejercicio de este derecho debe participar necesariamente el Ministerio Fiscal. Es fundamental indicar que cuando en la sentencia se declare la existencia de la vulneración, ésta irá necesariamente aparejada de una indemnización que deberá fijar el juez, tal y como establece el artículo 183 LRJS.

- Rescisión indemnizada del contrato por voluntad del trabajador: El Estatuto de los Trabajadores, en su artículo 50, señala la posibilidad de que el trabajador rescinda su contrato de forma voluntaria con indemnización cuando el empresario incumpla sus obligaciones de forma grave. Para hacer efectiva esta acción es necesaria la declaración de un órgano judicial admitiendo la extinción. Al igual que en el caso anterior, será el trabajador el que deba aportar pruebas suficientes

acerca del incumplimiento grave de obligaciones del empresario, en relación con sus datos personales.

El carácter indemnizatorio de ambas acciones hace posible su acumulación, ya que es la única forma de garantizar la indemnización completa. En este sentido se pronuncia el Considerando 146 RGPD, indicando que «Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos».

IV. CONTROL DE LA ACTIVIDAD LABORAL

El Estatuto de los Trabajadores en su precepto 20.3 faculta al empresario a tomar las medidas necesarias de vigilancia y control para comprobar el cumplimiento por el trabajador de sus obligaciones. Ahora bien, en el desarrollo de estos controles se ven involucrados infinidad de datos personales con los que la empresa debe guardar la diligencia debida. Algo común a todos los medios de control es la obligación de la empresa de utilizar los datos personales de forma exclusiva para la finalidad establecida por cada tratamiento. La AEPD establece que, con anterioridad a la implantación de una medida de control, la empresa debe de llevar a cabo tres juicios:

- Juicio de idoneidad: Debe comprobar si es adecuado para alcanzar el fin establecido.
- Juicio de necesidad: Debe comprobar que no existe una medida más idónea y que ponga menos en riesgo al trabajador para llegar al objetivo propuesto.
- Juicio de proporcionalidad: Debe asegurarse de que los beneficios que aporta la medida son mayores que los riesgos que supone llevarse a cabo.

En esta sección, se van a analizar las distintas formas de control y los riesgos y precauciones que debe tener el empleador en materia de datos personales. Para la correcta utilización. La AEPD establece la recomendación de que las empresas creen una Política Corporativa en la que establezcan de forma clara las distintas medidas de control que se van a utilizar y que deberá de mantenerse actualizada. Los empresarios deben asegurarse, además, de que los trabajadores conozcan y sean informados de dicha política.

1. Control informático y de las comunicaciones

Una gran mayoría de las empresas europeas y españolas ponen a disposición de sus trabajadores el uso de elementos informáticos (ordenadores, móviles, tabletas…) para el efectivo desarrollo de su actividad laboral. En el uso de estos aparatos, el trabajador vuelca habitualmente una gran cantidad de datos de carácter personal. Además, con cada vez más frecuencia, se permite el traslado de estos elementos a el domicilio de los trabajadores, lo que provoca una mayor inmersión de datos personales y un mayor riesgo a la intimidad del trabajador.

En la Política Corporativa de la empresa se debe establecer de forma clara los métodos de control que se vayan a establecer en torno a estos dispositivos. Se debe indicar

claramente al trabajador la permisibilidad en el uso, recomendándose a las empresas, para un mayor control en protección de datos, que circunscriba el uso de forma exclusiva a la prestación de los servicios.

Queda prohibido la monitorización continua de los aparatos usados por el empleado, de acuerdo con el artículo 29 del Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de trabajo sobre protección de datos.

A tenor de la doctrina establecida por el Tribunal Europeo de los Derechos Humanos (en adelante, «TEDH»*)*, la Sala de lo Social del TS y el Tribunal constitucional (en adelante, «TC»), el control de los medios informáticos se considerará lícito al ser una mediada idónea, necesaria y proporcional, siempre y cuando se informe de forma correcta y con anterioridad a uso a los trabajadores, que se va a llevar a cabo.

2. Control de la videovigilancia

La ley 5/2014, de 4 de abril, de Seguridad Privada (en adelante, «LSP»), en su artículo 42.1 define los servicios de videovigilancia como aquellos que: «consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas. ». Se considerarán, por tanto, como supuesto de videovigilancia las grabaciones que se realizan en el lugar de trabajo, como método de control de los trabajadores. La captación de estas imágenes supone la inclusión en la esfera de los datos personales como ha establecido el TEDH en diversas sentencias como la Sentencia 59320/00, de 24 junio de 2004.

Los artículos 22 y 89 LOPD, junto con la AEPD, regulan el tratamiento que se puede realizar de las imágenes que se obtienen a través de la videovigilancia. Se establecen una serie de requisitos acerca de cómo se debe de llevar a cabo la videovigilancia:

- No será necesario el consentimiento de los trabajadores, ya que se entiende el contrato de trabajo y el reconocimiento de las facultades de control señaladas en el artículo 20.3 ET como base legitimadora suficiente.
- A pesar de lo establecido en el punto anterior, si existe la obligación de informar al trabajador sobre este medida. En el caso de que un trabajador cometa un acto ilícito se entenderá como información suficiente la ubicación de un cartel informativo visible en el que se indique el tratamiento, el Responsable, la

posibilidad de ejercer los derechos. El cartel deberá tener un tamaño suficiente como para ser fácilmente visible por todos los interesados. Este tamaño deberá determinarse también atendiendo a la superficie de los espacios videovigilados, de forma que cuanto más amplio sea éste, mayor deberá ser el cartel. En este sentido, resulta de aplicación el artículo 7 de la Orden INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada, que establece que las dimensiones mínimas del cartel que anuncie las medidas de seguridad obligatorias deben ser 18x12 centímetros. Por ello, ha de entenderse que el cartel de videovigilancia debe tener estas dimensiones. Se establece una imagen ejemplo de cómo debe ser el cartel en el Anexo I.

- Se establece que la videovigilancia no se podrá usar junto a otra tecnología como puede ser el reconocimiento facial, al entenderse como desproporcionado, viéndose vulnerado el principio de proporcionalidad.
- Para la correcta aplicación del principio de minimización, el empresario debe asegurarse de cumplir con las siguientes circunstancias:
    - El número de cámaras debe limitarse a las exclusivamente necesarias.
    - Los monitores de grabación deben ser ubicados en lugares a los que, con carácter general, solo puedan acceder los vigilantes de seguridad.
- Resulta prohibida la instalación de sistemas de videovigilancia en áreas destinadas al descanso o asueto de los trabajadores.
- Únicamente en aquellos lugares donde la implantación suponga un escaso riesgo (comunidades de propietarios o pequeños establecimientos) no será necesaria llevar a cabo una Evaluación de Impacto. En el resto de los lugares se deberá realizar e implementar las medidas de seguridad necesarias para reducir los riesgos.
- Si la empresa decide ceder la gestión de las cámaras a un tercero, este será considerado como un Responsable del Tratamiento.
- Se pueden conservar las imágenes grabadas durante un mes, salvo en casos en las que se deban de poner a disposición judicial o policial.
- Únicamente se permite la grabación de sonidos en los supuestos en los que se acredite un riesgo mayor para la seguridad de las instalaciones o del personal.

3. Geolocalización

La geolocalización es un método de control del trabajador regulado en el artículo 90 LOPD en relación con el 20.3 ET, que permite conocer la ubicación del empleado a través de los vehículos o dispositivos electrónicos que se le han entregado para el desarrollo de su actividad laboral. Se trata de un método de control que se utiliza, de forma general, cuando los trabajadores llevan a cabo su jornada laboral en un lugar externo al centro de trabajo.

La base legitimadora del control del trabajador por geolocalización es el contrato laboral, sin ser necesaria la autorización del trabajador para su desarrollo. Sin embargo, si será obligatorio informar a los empleados de la existencia y características de este sistema y de que se va a llevar a cabo, así como de la posibilidad de ejercer los derechos de acceso, rectificación, limitación y supresión. En este sentido, hay que recalcar que no será necesario el consentimiento cuando se realice la geolocalización en dispositivos o vehículos cuando se usa es explícitamente personal, pero si lo será en los supuestos en los que se permite también un uso personal.

En este supuesto resulta especialmente importante el cumplimiento del principio de proporcionalidad ya que se han dado sentencias como la Sentencia de la Audiencia Nacional (en adelante, «SAN») 136/2019 de 6 de febrero, Sala de lo Social, que determinan el sistema de geolocalización como ilícito al no superar ese principio.

4. Registro de la jornada

La empresa debe controlar el horario de inicio y final de la jornada laboral, en el cumplimiento de la obligación legal establecida por el artículo 34.9 ET. Dado que a partir de estos registros se identifica a una persona en concreto, se produce un tratamiento de datos personales cuya base legitimadora, como ya hemos mencionado, será la obligación legal. Aunque, como en los casos anteriores, el trabajador tendrá la obligación de ser informado.

Los registros de la jornada deben ser lo menos invasivos posibles, almacenando únicamente los datos personales imprescindibles. El ET establece un periodo de conservación de 4 años, periodo tras el cual deben ser eliminados. Se otorga libertad a la empresa para establecer los registros en el formato que prefiera, pero deberán mantenerlo en un lugar que asegure la confidencialidad, evitando que personas no autorizadas

accedan a él. Estos registros, y, por ende, los datos personales que aparecen en ellos solo pueden ser accesibles por los trabajadores (obviamente, para respetar la privacidad, cada uno al suyo), sus representante y Entidades o Autoridades Públicas. Es habitual lo solicitud de acceso a los datos por parte de la Inspección de Trabajo y Seguridad Social que podrá acceder a los datos cuando lo solicite, a tenor del artículo 18 de la Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social (en adelante, «LOITSS»).

5. Control de Acceso

La AEPD indica la no necesidad de consentimiento de los trabajadores para establecer controles de entrada a las instalaciones de trabajo. Entiende la Agencia que este tratamiento viene legitimado por el propio contrato de trabajo en caso de que solo se pretenda el control de la prestación del trabajador, e incluso podría venir legitimizado por un interés legítimo del empleador si el objetivo fuese la protección de los bienes empresariales.

En el caso de que se usen los mismos métodos para el control de acceso que para el registro de la jornada, los datos deben eliminarse, como se ha indico en el apartado anterior a los 4 años de su obtención. En el caso de que se usen sistemas independientes y únicamente tenga una finalidad identificativa, no se almacenarán más datos por lo que no se registrará ningún periodo de supresión especial.

6. Control de falta de asistencia por enfermedad o accidente (Control del absentismo)

El artículo 20.4 ET permite controlar al empleador el estado médico de las personas que se ausentan de su puesto de trabajo por enfermedad o accidente, con la finalidad de verificar su situación.

Este supuesto no es igual al visto en el apartado 3.5.A) acerca del tratamiento de datos de salud en materia de prevención de riesgos laborales, aunque presenta ciertas similitudes. En este caso no será necesario el consentimiento del trabajador para llevar a cabo el reconocimiento con la consiguiente recogida de datos, aunque se le debe informar de forma muy precisa de que se pretenden verificar sus condiciones en base a precepto mencionado. Incluso se establece en el artículo 20.4 ET que la negativa del trabajador a

someterse a estos reconocimientos puede suponer la suspensión de derechos económicos existentes en estas situaciones.

La empresa únicamente estará legitimada para conocer si la persona está en condiciones de reincorporarse al puesto de trabajo o si no. Se permite que el control del absentismo lo lleve a cabo una empresa externa, así lo reconoce la sentencia del Tribunal Supremo STS 481/2018, de 25 de enero, Sala de lo Social . Esta compañía actuará como Responsable del tratamiento.

Tanto si se procede a la verificación del estado de salud por la propia empresa como si lo hace por una tercera empresa, e debe de tener en cuenta que se están tratando datos de categoría especial y por ende hay que tratarlos con mayor cuidado.

7. Detectives Privados

Otra forma de control a los trabajadores admitida por la AEPD es la utilización de detectives, así lo establece el artículo 48 LSP en relación con el 20.3 ET. Ahora bien, resulta especialmente imprescindible en este caso la correcta realización del juicio de proporcionalidad, llevando a cabo únicamente este método cuando no se observe otra menos lesivo para el empleado.

Encuentra su base legitimadora en el contrato de trabajo y resulta importante apuntar la prohibición establecida por el artículo 48.3 LSP de: «investigar la vida íntima de las personas que transcurra en sus domicilios u otros lugares reservados, ni podrán utilizarse 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. ».

El informe realizado por el detective tras la investigación debe seguir las normas establecidas del art 49 LSP. En relación con los datos personales, se indica que:

- Únicamente se deben hacer constar aquellos datos imprescindible para el objeto y finalidad de la investigación.
- Los video e imágenes obtenidos durante la investigación se deben guardar, al menos tres años.
- Solo podrán acceder a las investigaciones y, por ende, a los datos personales, el cliente (empleador en este caso) y los órganos judiciales o policiales si fuese necesario.

V. CONCLUSIONES

A modo de conclusión, a lo largo del trabajo se ha podido observar como la regulación sobre la protección de datos personales es extensa y muy completa.

En primer lugar, en el ámbito de los derechos del trabajador en materia de protección de datos, se puede observar como el empleado disfruta los derechos generales que tienen todas las personas en lo relacionado con la protección de datos, añadiendo derechos extra como puede ser el derecho a recibir la información debida.

Por otro lado, se ha observado como aparecen regulados prácticamente la totalidad de supuestos relacionados con la protección de datos personales que se pueden dar en el desarrollo de la actividad laboral. Esta especial protección sobre los datos personales en la relación laboral comienza incluso antes que la propia relación laboral, cubriendo la totalidad de actividades que se desarrollan y llegando hasta más allá de la extinción de la relación laboral, al tener que guardar los datos del trabajador durante el tiempo establecido.

Por último, en cuanto a los métodos de control, de igual manera también se encuentran regulados en su totalidad. En este ámbito resulta importante que la AEPD se mantenga actualizada, dado que las constantes evoluciones tecnológicas pueden llevar a nuevos medios de control, para los que será necesario establecer ciertas regulaciones.

En definitiva, el RGPD vigente desde 2018 ha supuesto una total revolución en el ámbito de la protección de datos. Las empresas se han enfrentado a un reto mayúsculo para dar cumplimiento en todos los ámbitos de su actividad a este Reglamento, a la LOPD y a las Guías e Informes de la Agencia, siendo la adaptación a todos los requerimientos de protección de Datos Personales en el ámbito laboral especialmente exigente.

VI. BILIOGRAFÍA

- Ayudaley. «Protección de Datos para empleados. Guía 2021». 2021. Disponible en: https://ayudaleyprotecciondatos.es/2020/12/01/proteccion-datos-empleados/
- Baz Rodríguez. J., *Privacidad y protección de datos de los trabajadores en el entorno digital*, Bosch, Madrid, 2019.
- Blázquez Agudo, E.M., «Aplicación práctica de la protección de datos en las relaciones laborales», Bosch, Madrid, abril 2018.
- Caballero Gutiérrez, J. «GDPR: *Qué son las bases legitimadoras y cuándo aplican*. Tech Policy. 25 de enero de 2019. Disponible en: https://jlcaballero.com/es/gdpr-que-son-las-bases-legitimadoras-y-cuandoaplican/#:~:text=1%20%C2%BFQu%C3%A9%20son%20las%20bases,es%20posible%20tratar%20datos%20personales
- Colabora. «Tratamiento de datos personales por parte de los representantes de las personas trabajadoras». 2021. Disponible en: https://coolabora.es/tratamiento-por-representatntes-trabajadores/#:~:text=c)%3A%20el%20empleador%20no,ET%20establece%20a%20la%20empresa
- Grupo Ático 34. «Cesión de datos a terceros». Disponible en: https://protecciondatos-lopd.com/empresas/cesion-datos-terceros/
- Iberley. «Cuantía de las sanciones en materia laboral». 19 de enero de 2022. Disponible en: https://www.iberley.es/temas/cuantia-sanciones-materia-laboral-4591
- Legalitas. «Los límites de la empresa para controlar a sus trabajadores». 20 de abril de 2022. Disponible en: https://www.legalitas.com/actualidad/que-puede-hacer-y-que-no-la-empresa-en-relacion-a-datos-personales-de-empleados
- Ministerio de Trabajo, Migraciones y Seguridad Social. «Guía sobre el Registro de Jornada». 2022. Disponible en: https://www.mites.gob.es/ficheros/ministerio/GuiaRegistroJornada.pdf
- Perramón, V., «Protección de datos en el registro de jornada laboral». Figueras Legal, 25 junio de 2021. Disponible en: https://figueras.legal/proteccion-de-

datos-en-el-registro-de-jornada-laboral/#:~:text=El%20registro%20de%20jornada%20laboral%20constituye%20un%20tratamiento%20espec%C3%ADfico%20de,de%20protecci%C3%B3n%20de%20datos%20personales.

- Tu Asesor Laboral, «Recogida y tratamiento de datos en la extinción del contrato de trabajo». 29 de junio 2021. Disponible en: https://www.tuasesorlaboral.net/categorias-estudio/temas-juridicos/874-recogida-tratamiento-datos-extincion-contrato-trabajo

VII. ANEXO


ZONA VIDEOVIGILADA
RESPONSABLE:
BOLBIAC, S.L. C/Maracaibo 8, 08030, Barcelona.
PUEDE EJERCITAR SUS DERECHOS DE PROTECCIÓN DE DATOS ANTE:
- Presencialmente o por correo postal en: C/Maracaibo 8, 08030, Barcelona.
- Por email: info@bolbiac.com
MÁS INFORMACIÓN SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES:
- Finalidades: Videovigilancia
- Legitimación: Interés público
- No se cederán datos a terceros salvo obligación legal
- Más info: https://bolbiac.com/politica-de-privacidad/