LÍMITES AL CONTROL EMPRESARIAL Y CAPACIDAD DE INTERVENCIÓN DE LA RLT ANTE EL TRATAMIENTO DE DATOS PERSONALES DE LOS TRABAJADORES Y TRABAJADORAS

CCOO industria

¿Por qué esta guía?

Son muchas las incógnitas, aunque en muchos casos ya tenemos pruebas de ello, del impacto de la digitalización de la economía en el ámbito laboral. Esta guía no pretende entrar en los efectos para la destrucción o creación de empleo, los cambios producidos en el trabajo a realizar o la cualificación requerida en el presente o a futuro para afrontar esta transformación que está teniendo distintas velocidades ya sea entre las actividades, incluso territorios o incluso empresas o en la participación sindical para una transición justa a la digitalización[1].

Para no hacer más extensa esta guía, aunque puede dar algunas indicaciones, dejamos de lado también las recomendaciones sindicales de actuación para el acceso y tratamiento de la información a la que tenemos derecho como RLT en cumplimiento de esta normativa.

Lo que pretende esta guía es dar herramientas de actuación a la Representación legal de los trabajadores y trabajadoras de CCOO **para garantizar y poner en valor un derecho fundamental que no suele ser tan valorado como otros, el de la protección de datos**. Derecho más amplio que el de la intimidad, ya que afecta a otras esferas de la personalidad de la persona trabajadora que debe tener derecho a mantener reservadas y que son vulnerables a los excesos de las empresas en el ejercicio de los derechos que le otorga la legislación.

Como veremos, la Ley Orgánica 3/2018, de Protección de datos personales y garantía de los derechos digitales (LOPDGDD) pretende reforzar el derecho a la intimidad e información, pero dada la falta de concreción del articulado, la insuficiencia de regulación y los problemas interpretativos que dará según está adelantando la doctrina, y la remisión a la negociación colectiva, será ahí donde deberemos incrementar y garantizar la privacidad e intimidad de los trabajadores y trabajadoras. No hay que olvidar que la utilización de dispositivos digitales para el ejercicio de control empresarial no sólo puede tener afectación al derecho de protección de datos, aunque aquí sólo lo abordaremos desde esta perspectiva sino al conjunto de las condiciones de trabajo e incluso a la salud de las personas trabajadoras.

Las altas sanciones a las que pueden verse sometidas las empresas por el incumplimiento de la normativa relativa a la protección de datos ha permitido ya la apertura de mesas de negociación en las empresas, sobre todo, en aquellas más grandes. Esta guía se ha realizado al objeto de ayudar en este proceso a la RLT independientemente del tamaño de la empresa, ya que los límites y obligaciones empresariales son de aplicación a todas y cada una de las empresas que operan en nuestro país.

[1] Sobre esta materia, se puede consultar el documento "Reforzar la participación sindical para una transición justa a la digitalización" elaborado por la Secretaría de Acción Sindical de CCOO.

ÍNDICE

Aspectos generales de la protección de datos

La protección de datos como derecho fundamental. Evolución del marco normativo

Como dice en su *Preámbulo* la LOPDGDD, la protección de las personas físicas en relación con el tratamiento de datos personales es un **derecho fundamental protegido por el artículo 18.4 de la Constitución española (CE)**.

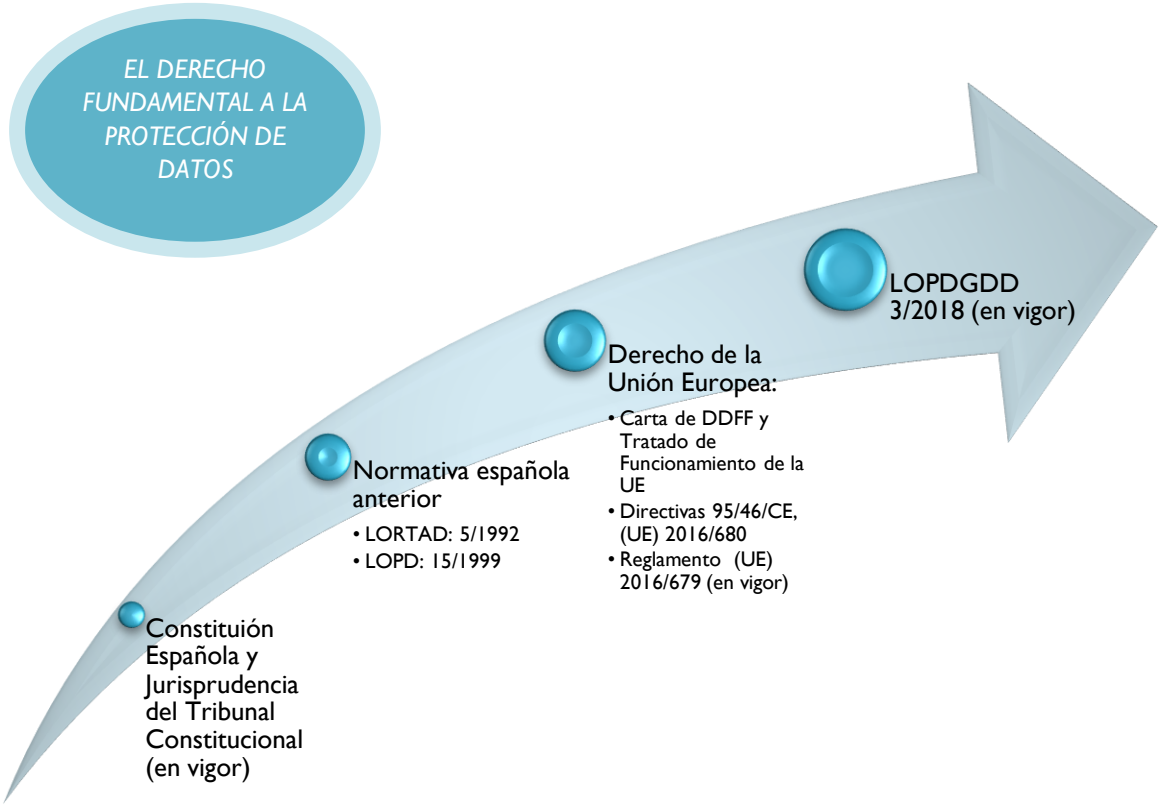
El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el **control sobre sus datos,** cualesquiera datos personales, y sobre **su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados**; de esta forma, el derecho a la protección de datos se configura como una **facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención**. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un **poder de disposición y de control sobre los datos personales** que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea.

En 2016 se aprobó el **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 sus datos personales y a la libre circulación de estos datos** y por el que se deroga la Directiva 95/46/CE.

La adaptación al Reglamento general de protección de datos, que es aplicable desde el 25 de mayo de 2018, según establece su artículo 99, provocó, aunque no fuera necesario, porque es de aplicación directa, la elaboración de una nueva ley orgánica que sustituyera la Ley Orgánica de 1999. Así se llegó ley orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales, en adelante LOPDGDD.

El artículo 8, apartado 1, de la Carta de Derechos Fundamentales de la Unión Europea el artículo 16, apartado 1, del Tratado de funcionamiento de la Unión Europea establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan



En esta guía, nos centraremos en la regulación establecida en el Reglamento y que es de aplicación inmediata en nuestro ordenamiento jurídico, haciendo alusión a la LOPDGDD cuando complete algunas de las estipulaciones recogidas en la norma europea.

Objeto (Art. 1.1y 1.2 Reglamento y art. 1 c) LOPDGDD)

¿Qué pretende proteger esta normativa?

Establece las normas relativas a la protección de las personas físicas en lo que respecta al **tratamiento** de **datos personales** y las normas relativas a la libre **circulación** de tales datos.

Protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de datos personales.

Garantiza los **derechos digitales** de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución

Datos personales: toda información sobre una persona física identificada o identificable (**interesado /a**). 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.

La Agencia Española de Protección de datos y la Jurisprudencia ha considerado datos personales, entre otros: la fotografía en las tarjetas identificativas de los trabajadores/as; el registro de tiempo de trabajo; la grabación de la imagen y/o sonido de una persona trabajadora o no de la empresa; la indicación de que un trabajador/a está en situación de baja temporal; las evaluaciones y juicios subjetivos; dirección de correo electrónico o de IP; el historial de accesos a internet; la titulación académica, la dirección postal; el número de teléfono móvil.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de 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;

Derechos digitales: El titulo X de la LOPDGDD desarrolla una parte del objeto de la ley, relativa a la garantía de derechos digitales. Según el art. 79, los derechos de la era digital son los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Enumera alguno de ellos en los siguientes artículos:

Artículo 80. Derecho a la neutralidad de Internet. Artículo 81. Derecho de acceso universal a Internet. Artículo 82. Derecho a la seguridad digital. Artículo 83. Derecho a la educación digital. Artículo 84. Protección de los menores en Internet. Artículo 85. Derecho de rectificación en Internet. Artículo 86. Derecho a la actualización de informaciones en medios de comunicación digitales. *Artículo 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral. Artículo 88. Derecho a la desconexión digital en el ámbito laboral. Artículo 89. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Artículo 91. Derechos digitales en la negociación colectiva.* Artículo 92. Protección de datos de los menores en Internet. Artículo 93. Derecho al olvido en búsquedas de Internet. Artículo 94. Derecho al olvido en servicios de redes sociales y servicios equivalentes. Artículo 95. Derecho de portabilidad en servicios de redes sociales y servicios equivalentes. Artículo 96. Derecho al testamento digital.

Derechos de la persona interesada (capítulo III del Reglamento y Capítulo II LOPDGDD)

Derecho	¿En qué consiste?
ACCESO	Derecho a conocer la finalidad del tratamiento, la persona responsable, categoría de datos personales que se traten, posibles comunicaciones de datos y sus destinatarios, el tiempo de conservación (si es posible) o los criterios para su determinación.
RECTIFICACIÓN	Derecho a rectificar los datos inexactos, a completar los datos personales incompletos incluso mediante declaración adicional
SUPRESIÓN (DERECHO AL OLVIDO)	Derecho a solicitar la supresión de datos personales sin dilación debida. Por ejemplo, cuando haya desaparecido la finalidad que motivó su recogida.
LIMITACIÓN DE TRATAMIENTO	Derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones establecidas.
PORTABILIDAD	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 (incluso de responsable a responsable) sin que lo impida el responsable al que se los hubiera facilitado
OPOSICIÓN	Derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento.
A NO SER OBJETO DE DECISIONES INDIVIDUALIZADAS	Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Se tendrá que tener en cuenta que estos derechos también se encuentran limitados por otros, por lo que se tendrá que estar a la normativa en cada caso.

Principios relativos al tratamiento (Art. 5 Reglamento)

Los datos personales serán:

¿Cómo debe tratar la empresa esos datos?

Tratados de manera lícita, leal y transparente en relación con el interesado («**licitud, lealtad y transparencia**»);

Recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; (…) («**limitación de la finalidad**»);

Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («**minimización de datos**»);

Exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («**exactitud**»);

Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (…). («**limitación del plazo de conservación**»).

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**»).

Si se da el teléfono personal para estar localizable en un proceso de selección, ese consentimiento no serviría para contactar con la persona trabajadora una vez hubiera entrado en la empresa.

Los datos de afiliación no deben servir para hacer el descuento en una huelga general.

Artículo 5 LOPDGDD. Deber de confidencialidad. 1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679. 2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable. 3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

El responsable del tratamiento [2]será responsable de que los datos se han tratado de manera lícita, leal y transparente y debe ser capaz de demostrarlo («**responsabilidad proactiva**»).

El principio de proporcionalidad

El tratamiento de los datos debe ser proporcional al objetivo perseguido. Aunque la LOPDGDD no hace mención expresa a este principio -aunque el artículo 5, indirectamente hace alusión al mismo- la jurisprudencia del Tribunal Constitucional se ha pronunciado sobre la extensión de este principio. La guía que editó la Agencia Española de Protección de Datos en 2009, también hacía referencia al mismo.

¿Cuándo puede tratar datos personales la empresa?

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

[2] La normativa regula la figura del encargado y del responsable del tratamiento. En el primer caso, se trata de la persona, autoridad pública, servicio u organismo que trate los datos personales por cuenta del responsable, y éste, es quien determina los fines y medios del tratamiento.

1. Si tal medida es susceptible de conseguir el objetivo propuesto (juicio de **idoneidad**).
2. 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**).
3. Y, 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).

Licitud del tratamiento (Art. 6 Reglamento).

El tratamiento **solo será lícito** si se cumple al menos una de las siguientes condiciones:

a) la persona interesada dio su *consentimiento* para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es *necesario para la ejecución de un contrato* en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento *es necesario para el cumplimiento de una obligación legal* aplicable al responsable del tratamiento;

d) el tratamiento es necesario para *proteger intereses vitales* del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada *en interés público* o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

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

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

STS 21 de septiembre de 2015.. Se establece la nulidad de una cláusula tipo del contrato de trabajo en la que se hace constar la posibilidad de que la empresa pueda efectuar comunicaciones al trabajador vía SMS o vía correo electrónico, según los datos facilitados por el trabajador a efectos de contrato, con la obligación, además, de comunicar a la empresa de forma inmediata cualquier cambio o incidencia en el teléfono o en el correo electrónico.

Sería ilícito que la empresa enviara un mensaje de texto al número de teléfono personal felicitando al trabajador o trabajadora su cumpleaños.

Conforme al Considerando 47 del Reglamento, la existencia de un interés legítimo requerirá una **evaluación meticulosa** en el momento y en el contexto de la recogida de datos personales (incluso si el interesado puede prever de forma razonable que puede producirse el tratamiento para tal fin).

A modo de ejemplo, no es necesario consentimiento de los trabajadores y trabajadoras:

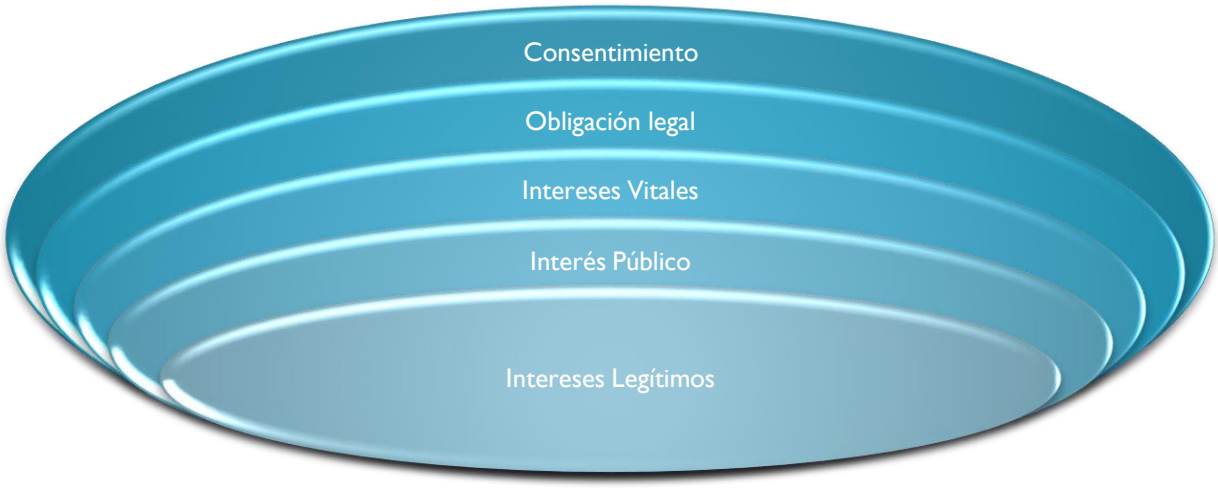
Para que la RLT pueda acceder a los datos sobre el registro de jornada previsto en el art. 34 del Estatuto.

Cuando el empresario adopte medidas de vigilancia y control al venir recogido en el art. 20.3 Estatuto, para verificar el cumplimiento por el trabajador/a de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad

Para la cesión de datos que han de proporcionarse a la Administración Pública en materia Tributaria o de seguridad social

Para la cesión de datos contenidos en la copia básica del contrato o datos de la empresa contratista a la RLT (8.4 y 42.3 ET)

Información relativa a las conclusiones de los reconocimientos médicos en materia de Prevención de Riesgos Laborales (22 LPRL)



Condiciones para el consentimiento (Art. 7 Reglamento)

Artículo 6 LOPDGDD. "1. (...) se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. 2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas. 3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

Cuando sea necesario, ¿cómo tiene que ser el consentimiento?

- El responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
- La solicitud de consentimiento se debe haber presentado de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.
- La persona interesada tendrá derecho a retirar su consentimiento en cualquier momento. Será tan fácil retirar el consentimiento como darlo.
- Antes de dar su consentimiento, la persona interesada será informado de ello.
- El consentimiento tiene que darse libremente, sin que se pueda supeditar la ejecución de un contrato, incluida la prestación de un servicio, al consentimiento de datos personales no necesarios.

EL CONSENTIMIENTO EN EL ÁMBITO LABORAL

El GT29 (grupo de trabajo de autoridades de los Estados Miembros en protección de datos del artículo 29 del Reglamento), en su dictamen 15/2011 dejó sentado que el recurso al consentimiento deberá limitarse a los casos en los que el trabajador/a pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello. En su dictamen 2/2017 ha subrayado que en la práctica, el consentimiento es una condición de ***"legitimación excepcional"*** *para el empleador, ya que por lo general, el trabajador/a no está en condiciones de prestar un consentimiento válido dadas las circunstancias.*

Además, hay que tener en cuanto lo previsto en el art. 9. 1 Reglamento sobre el consentimiento ***explícito*** *en el caso de* ***categorías especiales de datos personales****. Se pretende evitar la creación de listas negras.*

Cuando no sea necesario consentimiento pero se dé otra circunstancia de licitud del tratamiento, en todo caso, deberá hacerse efectivo el derecho de información al trabajador o trabajadora. *Por ejemplo, el caso de las cámaras de videovigilancia.*

Información que deberá facilitar la persona responsable del tratamiento a la persona interesada[3] (Artículo 13 y 14 del reglamento)

Y si el consentimiento no es necesario ¿La empresa no tiene ninguna obligación?

- La existencia del fichero o tratamiento, su finalidad y personas destinatarias.
- El carácter obligatorio o no de la respuesta y sus consecuencias.
- La posibilidad de ejercitar los derechos de acceso, rectificación, acceso, cancelación y oposición.
- La identidad y datos de contacto del responsable del tratamiento.
- Los datos de contacto del Delegado de Protección de Datos.
- La base jurídica o legitimación para el tratamiento.
- El plazo o los criterios de conservación de la información
- La existencia de decisiones automatizadas o elaboración de perfiles
- La previsión de transferencias a terceros países
- El derecho a presentar una reclamación ante las Autoridades de control

Y además si los datos no se obtienen de la persona interesada:

- El origen de los datos
- Las categorías de los datos

En el último apartado hablaremos también del derecho de información en casos concretos como en el de sistemas de geolocalización, entre otros.

Tratamiento de categorías especiales de datos personales (Art.9 Reglamento)

¿Puede tratar datos como la afiliación sindical?

Quedan **prohibidos** el tratamiento 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 la orientación sexual de una persona física.

No obstante, esta norma general **no se aplica,** entre otros, en los siguientes casos:

- ✓ la persona interesada dio su **consentimiento explícito** para el tratamiento de dichos datos personales con uno o más de los fines especificados,
- ✓ 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, con los límites que establece el reglamento.

[3] Las empresas tienen a su disposición en https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf la guía para el cumplimiento del deber de informar de la Agencia Española de Protección de Datos.

- ✓ el tratamiento es necesario para proteger **intereses vitales** de la persona interesada o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
- ✓ el tratamiento es 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, con los límites que establece el reglamento;
- ✓ 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,** con los condicionantes del art. 5.
- ✓ el tratamiento, si se hace conforme establece el artículo, es necesario para fines de **medicina preventiva o laboral, evaluación de la capacidad laboral** del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.
- ✓ el tratamiento es necesario por razones de interés público en el ámbito de la **salud pública**, sin perjuicio de otras garantías.
- ✓ el tratamiento es necesario con fines de **archivo en interés público**, fines de **investigación** científica o histórica o fines estadísticos, con los límites del artículo 5.

El mismo reglamento obliga a la **normativa nacional a establecer garantías adicionales en esta materia.**

Organismos con competencias en materia de protección de datos

Comité Europeo de Protección de datos (antes Grupo de Trabajo del artículo 29 del Reglamento)

El CEPD es un organismo de la Unión Europea (UE) responsable de la aplicación del Reglamento general de protección de datos (RGPD) a partir del 25 de mayo de 2018. Está compuesto por el director de cada autoridad de protección de datos (APD) de cada estado miembro y el Supervisor Europeo de Protección de Datos o sus representantes. La Comisión Europea participa en las reuniones del CEPD sin derecho a voto. La secretaría del CEPD estará a cargo del Supervisor Europeo de Protección de Datos.

En el artículo 70 se encuentran las funciones que se le atribuye a este organismo entre las que se encuentra la emisión de directrices, recomendaciones y buenas prácticas.

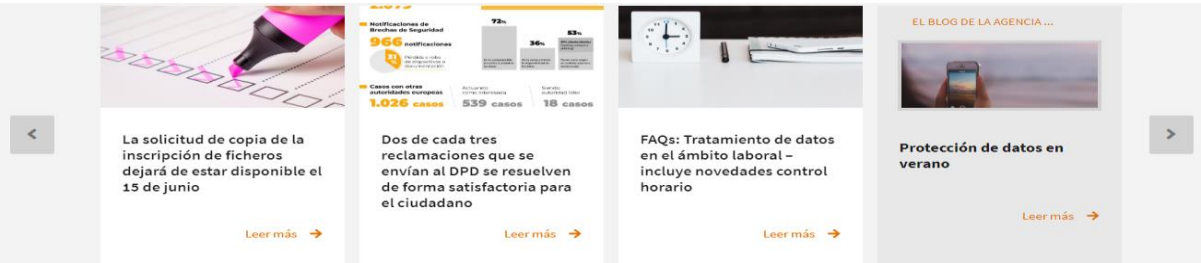
En el último apartado de esta guía se pueden consultar las guías del grupo de trabajo del artículo 29

Agencia Española de Protección de datos

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de la LOPDGDD y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la ley orgánica y en sus disposiciones de desarrollo. También le corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Tiene, entre otras funciones, la de controlar la aplicación del Reglamento y hacerlo aplicar o previa solicitud, facilitar información a cualquier persona interesada en relación con el ejercicio de sus derechos; tratar las reclamaciones presentadas por un interesado/a o por un organismo, organización o asociación, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

Dentro de sus competencias, ha elaborado una serie de guías e indicaciones que se pueden consultar en www.aepd.es. Además, a raíz de la publicación de la ley, ha publicado sus principales novedades.



Preguntas que la AEPD ya ha resuelto en www.sedeaed.gob.es

¿Te atreves a responder?

- ¿PUEDEN CONTENER DATOS DE SALUD LOS JUSTIFICANTES DE AUSENCIA LABORAL?
- ACCESO DEL COMITÉ DE EMPRESA A UN LISTADO DE LAS PERSONAS TRABAJADORAS BENEFICIARIAS DE LA ACCIÓN SOCIAL.
- LAS TARJETAS IDENTIFICATIVAS DE LOS TRABAJADORES ¿PUEDEN INCLUIR NOMBRE, APELLIDOS Y DNI?
- VULNERA LA NORMATIVA DE PROTECCIÓN DE DATOS UTILIZAR UN SISTEMA DE FICHAJE USANDO EN LA APLICACIÓN DE UNA FUNCIÓN NUMÉRICA A CADA EMPLEADO FUNDADA EN UN ALGORITMO GENERADO POR SU HUELLA DIGITAL?
- ¿PUEDEN CEDERSE LOS DATOS DE SALARIOS Y TC2 DE UNA SUBCONTRATA A LA EMPRESA PRINCIPAL?
- ¿SE PUEDE INSTALAR GPS EN LOS COCHES DE EMPRESA QUE UTILIZAN LOS TRABAJADORES?
- ¿SE PUEDEN SOLICITAR LOS ANTECEDENTES PENALES PARA UN PUESTO DE TRABAJO?
- ¿ES FACTIBLE COMUNICAR LOS RESULTADOS DE RECONOCIMIENTOS MÉDICOS AL EMPRESARIO, COMITÉ DE EMPRESA Y SECCIÓN SINDICAL?
- ¿ES NECESARIO EL CONSENTIMIENTO DEL TRABAJADOR O TRABAJADORA PARA IMPLANTAR UN SISTEMA DE CONTROL HORARIO? ¿HAY QUE INFORMARLE ACERCA DE LAS MEDIDAS DE CONTROL ESTABLECIDAS?
- EN EL CASO DE QUE SE TRABAJE CON PROVEEDORES, ¿CÓMO SE ESTABLECE ESA RELACIÓN PARA EL CONTROL HORARIO?
- ¿PUEDE SOLICITAR EL EMPRESARIO EL TELÉFONO Y DIRECCIÓN DE CORREO ELECTRÓNICO PARTICULAR DEL TRABAJADOR?

Tienes las respuestas en la página 25.

Además debemos hacer referencia a las **Agencias Autonómicas** con competencias en materia de protección de datos:

- Autoridad catalana de protección de datos.
- Agencia vasca de protección de datos.
- Consejo de transparencia y protección de datos de Andalucía.

Otras cuestiones

El ejercicio de las facultades de la Representación Legal de los Trabajadores y Trabajadoras

Es habitual que la empresa niegue determinada información a la RLT alegando que la misma contiene datos personales de las personas trabajadoras de la empresa o información confidencial de la misma.

Como veremos con posterioridad, los poderes de dirección de la empresa no son ilimitados y la empresa no puede utilizar el derecho a la protección de datos para obstaculizar el ejercicio de los derechos de información de la RLT.

La jurisprudencia, además, ha declarado, que es lícita la comunicación por parte de la empresa a los representantes de las personas trabajadoras de datos personales necesarios para el ejercicio de las competencias que se les atribuyen legal o convencionalmente (STS 7-2-18). Lógicamente, al hablar de datos personales de la plantilla, su tratamiento deberá estar sometido a lo establecido en la normativa vigente y en concreto en la LOPDGDD (artículo 5, **Deber de confidencialidad**, por ejemplo).

> ***La empresa no puede alegar la LOPDGDD o la Ley de Secretos empresariales 1/2019 si esto limita la autonomía colectiva o el derecho de la RLT a la negociación colectiva, aunque todo tratamiento de datos personales que realice, estará sometida a lo que diga esta normativa.***

En cualquier caso, hay que recordar el artículo 65 del Estatuto de los Trabajadores. "2. *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. 3. En todo caso, ningún tipo de documento entregado por la empresa al comité podrá ser utilizado fuera del estricto ámbito de aquella 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. 4.* ***Excepcionalmente****, la empresa no estará obligada a comunicar aquellas informaciones específicas relacionadas con secretos industriales, financieros o comerciales cuya divulgación pudiera, según criterios objetivos, obstaculizar el funcionamiento de la empresa o del centro de trabajo u ocasionar graves perjuicios en su estabilidad económica. Esta excepción no abarca aquellos datos que tengan relación con el volumen de empleo en la empresa*".

Sobre este apartado 4, tenemos que recordar el artículo 1.3 de la Ley de Secretos Empresariales que establece "*La protección de los secretos empresariales no afectará a la autonomía de los interlocutores sociales o a su derecho a la negociación colectiva. Tampoco podrá restringir la movilidad de los trabajadores; en particular, no podrá servir de base para justificar limitaciones del uso por parte de estos de experiencia y competencias adquiridas honestamente durante el normal transcurso de su carrera profesional o de información que no reúna todos los requisitos del secreto empresarial, ni para imponer en los contratos de trabajo restricciones no previstas legalmente*".

Más adelante veremos las concretas facultades que tiene la RLT para garantizar el derecho a la intimidad de las personas trabajadoras en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización.

Sistemas internos de denuncias (Art. 24 LOPDGDD)

La LOPDGDD establece la licitud del tratamiento de datos, sin que sea necesario el consentimiento, en los sistemas de denuncias internas, incluso anónimas, por ejemplo, en los protocolos internos de denuncia de los casos de acoso sexual y por razón de sexo (art. 48 LO 3/2007), en la prevención de delitos en la empresa (art. 31 bis CP) o de blanqueo de capitales (RDL 11/2018). No obstante, el artículo establece una serie de limitaciones:

- Su tratamiento sólo podrá hacerse por el personal de interno que desarrollen funciones de control interno y de cumplimiento o a los encargados designados o también aquellas personas de la empresa o externas y sólo al personal con funciones de gestión cuando se pudiera proceder a la adopción de medidas disciplinarias.
- Los datos sólo deben guardarse por el tiempo imprescindible sobre la procedencia del inicio de la investigación y en todo caso, 3 meses, salvo que la finalidad de su conservación sea la de dejar evidencia del funcionamiento del modelo.
- Pasados los 3 meses sólo podrán seguir tratándose los datos conforme al apartado 2, no conservándose en el propio sistema de medidas internas.

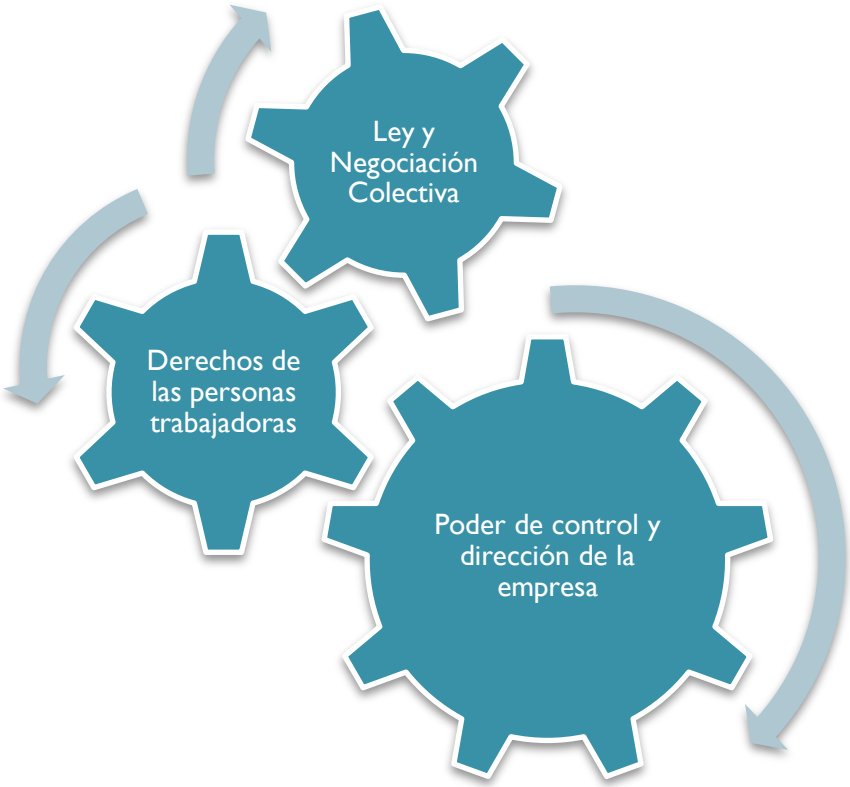
En la guía que publicó la AEPD en 2009 ya hacía alusión a esta posibilidad y establecía una serie de recomendaciones:

- Información previa de su existencia y las consecuencias para la persona denunciada.
- Respeto del principio de proporcionalidad: especificando qué acciones deben ser objeto de denuncia y especificando las normas legales o códigos internos de conducta a las que se refieren.
- Garantizar el deber de secreto y que el denunciado no conozca la identidad del denunciante.
- Notificación de estos ficheros al registro general de Protección de datos.

La utilización de nuevas tecnologías en el marco de relaciones laborales. Límites empresariales y derechos de las personas trabajadoras y de su Representación Legal

El artículo 20 del Estatuto de los Trabajadores define el **poder de control y Dirección de la Empresa** pero también sus límites.

En concreto en el art. 20.3 establece "*El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad*".



Por otro lado, el artículo 20 bis recoge "*Los trabajadores tienen* ***derecho a la intimidad*** *en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales*".

Como estableció en su artículo 88 del Reglamento "1. *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 empleados 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. 2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales*

dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo (…)".

Por su parte, la LOPDGDD, desarrolla, sin entrar en profundidad y sin dar todas las garantías necesarias, según entendemos, el derecho a la intimidad y a la desconexión digital y el derecho y límites al control empresarial en el uso de dispositivos puestos a disposición por la empresa, sistemas de videovigilancia y grabación de sonidos y sistemas de geolocalización.

	Derechos y obligaciones para la empresa	**Derechos y obligaciones para la RLT y las personas trabajadoras**
Dispositivos digitales puestos a disposición de la persona trabajadora por la empresa (art. 87)	• **Acceso de la empresa a contenidos** sólo para controlar el cumplimiento de las obligaciones laborales o estatutarias y garantizar la integridad de los dispositivos. • Debe elaborar unos **criterios** de utilización. • Estos criterios deben cumplir unos estándares mínimos de protección de su intimidad conforme a los usos sociales y derechos. • Para el acceso, los criterios deben especificar los usos autorizados y las garantías para preservar la intimidad así como los períodos en que se pueden utilizar para usos privados.	• Derecho a la **protección** de su intimidad en el uso de esos dispositivos. • En la elaboración de los **criterios** deberá **participar** la **RLT**. • Se deberá **informar** a las personas trabajadoras de los criterios de utilización.

Desconexión digital (art. 88)	• Las **modalidades de su ejercicio** potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar
	  ○ Se sujetarán a lo establecido en la **Negociación Colectiva.**
	  ○ En su defecto, a lo acordado entre la RLT y la empresa.
	• En todo caso, la empresa elaborará una **política interna** en la que definirán:
	  ○ Modalidades de ejercicio
	  ○ Acciones de formación y sensibilización del personal sobre un uso razonable de las herramientas informáticas que evite el riesgo de fatiga informática.
		• Garantizar, fuera del tiempo de trabajo, el **respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar**.
		• Debe existir **audiencia previa de la RLT** en la elaboración de la política interna.

Dispositivos de videovigilancia	• **Tratamiento de imágenes** para el ejercicio de las funciones de	• Derecho a la **intimidad**. • La empresa debe **informar**

y de grabación de sonidos en el lugar de trabajo (art. 89)	control del art. **20.3 ET,** siempre que se ejerzan dentro de su marco legal y con sus límites. • **Prohibición** de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de la plantilla: vestuarios, aseos, comedores y análogos. • La utilización de sistema similares para la **grabación de sonidos**, se admitirá, **únicamente:** ○ cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrollo en el centro de trabajo. ○ Respetando el principio de proporcionalidad, intervención mínima y garantías previstas en los apartados anteriores.	**previamente** de forma **expresa, clara y concisa** a las personas trabajadoras y a la RLT, en su caso, acerca de esta medida. Se entiende cumplido el deber de informar en caso de captación flagrante de un acto ilícito y si estaba en un lugar lo suficientemente visible y constaba la identidad del responsable y dirección del ejercicio de derecho. La supresión de sonidos conservados por estos sistemas de grabación deben cumplir lo previsto en el artículo 22.3 de la LOPDGDD.
Sistemas de geologalización (art.90)	• Posibilidad de tratamiento para el ejercicio de de las funciones de control del 20.3 ET, siempre que se ejerzan dentro de su marco legal y con sus límites.	• Derecho a la **intimidad**. • La empresa debe **informar** de forma expresa, clara e inequívoca a las personas trabajadoras y su RLT acerca de la existencia y característica de estos dispositivos y del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

En todo caso, no hay que olvidar lo ya comentado sobre la aplicación del **principio de proporcionalidad**, ya que el tratamiento de datos personales afecta directamente a derechos fundamentales.

A estos límites al poder del empresario hay que añadir lo previsto en el artículo 91 LOPDGDD *"**Los convenios colectivos podrán establecer garantías adicionales** de los derechos y libertades relacionadas con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral"*.

En el apartado Resoluciones Judiciales relativos a los derechos individuales de las personas trabajadoras se puede ver el extracto de las principales sentencias en esta materia. Deberemos tener en cuenta los vaivenes judiciales y la falta de unificación de doctrina en algún aspecto como en el de licitud de las pruebas.

Dispositivos digitales puestos a disposición de la persona trabajadora por la empresa

¿Qué podemos considerar dispositivos digitales?

Cuando hablamos de estos dispositivos nos referimos a todo mecanismo destinado a la generación, transmisión, manejo, procesamiento y almacenamiento de señales **digitales,** sean móviles o no. Hablamos de PCs y portátiles, teléfonos móviles, "weareables" etc.

¿Qué deben respetar los criterios a los que hace referencia el artículo 87?

Como hemos visto, todo trabajador y trabajadora tiene derecho a la **protección de datos de carácter personal**. Se trata de un derecho fundamental autónomo e independiente, aunque está directamente relacionado con otros como el derecho a la **intimidad** o la dignidad de la persona, al honor o puede afectar al de igualdad o incluso el de libertad sindical.

Además, las comunicaciones de las plantillas en la empresa a través de los sistemas de comunicación propiedad del empresario/a, con independencia del sistema de comunicación elegido (postal, teléfono, fax, correo electrónico...), están protegidas por el **derecho fundamental al secreto a las comunicaciones**. Indica el art. 18.3 CE que "*se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*". Como luego veremos, además, entronca con un nuevo derecho, el de la **desconexión digital**.

Como hemos visto, sin embargo, el tratamiento de datos de carácter personal puede ser lícito aunque también tiene sus límites. Debe aplicarse el principio de **proporcionalidad**, se debe **informar** a la plantilla, por lo que la información será siempre **previa** al uso (sobre finalidad del tratamiento, duración de la conservación de los datos obtenidos, seguridad de los datos de conexión y archivo de los mensajes electrónicos profesionales) y **participar la RLT** en su elaboración. Además, en ningún caso, la finalidad puede ser otra diferente a la del 20.3 ET cumpliendo el **tratamiento** de datos debe cumplir lo establecido en la LOPDGDD.

> ***"Cuando hay una prohibición expresa y válida del uso personal y no hay expectativa razonable de intimidad, es lícito probar la desobediencia a través de la monitorización del ordenador del trabajador. Y más si el control está justificado en la información previa obtenida lícitamente por la empresa sobre el incumplimiento del trabajador y fue proporcionado, no genérico, al realizarse desde el servidor de la empresa, en determinadas fechas y en relación con el incumplimiento del código de conducta" STS 8-2-18.***
>
> ***"No hay lesión de la intimidad por la comprobación de un soporte informático de uso común (TCO 241/2012); ni por analizar criterios clasificados en el ordenador del trabajador como "datos personales", cuando las instrucciones de la empresa indican específicamente que la información privada debe estar claramente identificada como "privado"" (TEDH 22-2-18).***

El Documento de trabajo del GT29, relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo con relación al uso de internet, se ha pronunciado al respecto, tanto del uso de internet con fines privados como al eventual tratamiento de datos personales relativos a **páginas de internet consultadas por la plantilla**. En este último caso considera que "convendría acudir preferiblemente a medidas preventivas como la instalación de filtros que puedan impedir ciertas operaciones y, asimismo, prevenir a los trabajadores –y trabajadoras- de los controles que puedan realizarse de sus datos personales, efectuados preferiblemente, de forma graduada y por prospecciones no individualizadas, utilizando datos anónimos o de alguna forma desagregados".

El GT29, también se ha pronunciado sobre la utilización de herramientas propias de la persona trabajadora para el uso laboral, lo cual debemos evitar. "Para evitar el control de la información privada, deben establecerse medidas adecuadas para distinguir entre el uso privado y corporativo del dispositivo. Para ello, los empleadores también deben implementar métodos por los cuales sus propios datos sean transferidos de forma segura entre esos dispositivos y su red. Así, se podría configurar el dispositivo para enrutar todo el tráfico a través de una VPN, lo que permitiría ofrecer un cierto nivel de seguridad"

¿Qué podemos hacer como RLT?

Da la sensación que la normativa inclina la balanza a favor de las facultades del empresario/a que le atribuye el artículo 20 ET, por encima de los derechos fundamentales a los que hemos hecho referencia.

Hoy en día ya existen códigos de conducta implantados de manera unilateral por la empresa que establecen cómo deben usarse los dispositivos digitales por parte de los trabajadores y trabajadoras. En la mayoría de ocasiones, los incumplimientos de la plantilla de las indicaciones en ese código, sean más o menos abusivas, han pretendido utilizarse por parte de las empresas para sancionar a las personas trabajadoras.

Debe tenerse en cuenta que el principio de tipicidad de las sanciones disciplinarias hace que éstas solamente sean válidas si se han previsto en convenio colectivo.

Por ello, cabe dudar de la legalidad de algunas de las cláusulas contenidas en dichos códigos de conducta interno.

Diversas sentencias señalan respecto a la utilización del correo electrónico, por ejemplo que existe vulneración del deber de buena fe sancionable, la utilización abusiva del correo electrónico con finalidades extraproductivas. No obstante lo anterior, lo más probable es entender que la sancionabilidad de la conducta dependerá de la existencia de una **clara política empresarial** sobre esta materia **conocida** por los trabajadores y trabajadoras. De ahí, que la ley también exija que las personas trabajadoras conozcan fehacientemente las restricciones empresariales que se imponen al uso del correo electrónico, aunque no lo contemple el convenio colectivo.

Asimismo, debe tenerse en cuenta que el uso indebido del correo electrónico sancionable no solamente se extiende a la utilización con finalidades personales del correo electrónico, sino también puede incluir otras conductas ilícitas que se realizan a través del correo electrónico. Tal sería el caso, por ejemplo, de los envíos de información confidencial de la empresa o del hostigamiento o acoso sexual a través de correo electrónico, como puede ser enviar material sexualmente explícito o comentarios de contenido sexual a otros trabajadores en la empresa. Sobre este particular la incipiente doctrina judicial es tajante al indicar que conductas como las descritas constituyen una modalidad de acoso sexual sancionable (STSJ Cataluña 5-7-2000).

Dicho esto, parece que la negociación de los criterios de uso de los dispositivos o las cláusulas que recogieran los Convenios Colectivos deberían garantizar y recoger lo siguiente:

- El principio de proporcionalidad y el derecho de transparencia e información con las mayores garantías.
- Evitar la sanción automática del trabajador o trabajadora por entender arbitrariamente la empresa que se ha incumplido los criterios establecidos. Puede ser positivo desde la obligación de la comunicación previa a la RLT de cualquier tipo de sanción, a la creación de una comisión que analice una situación que la empresa entienda sancionable o cuando haya que actualizar los procedimientos a esta normativa.
- No debería poder ser sancionable el incumplimiento de una recomendación u obligación que imponga la empresa en esta materia que no ponga en grave riesgo a la compañía o que exceda no sólo el principio de proporcionalidad, sino las recomendaciones que realice la AEPD[4].
- El convenio colectivo, en ningún caso, deberá limitar los derechos que la RLT tenga para el ejercicio de sus funciones. Al contrario, deberá garantizar el uso de estos dispositivos para la acción sindical.
- La formación en esta materia, que deberá realizarse en horario laboral, debería ser conocida previamente por la RLT para garantizar que se ajusta a lo establecido legalmente.
- Extensión de estas garantías más allá de la empresa principal.
- Garantizar el derecho a la desconexión.

Desconexión Digital

La necesidad de conciliar, tal y como aparece en la norma, y en menor ocasión, los daños a la salud laboral que la sobreexposición a las nuevas tecnologías pueden provocar, se están recogiendo con justificadoras, en la mayoría de los casos, del reconocimiento de este derecho, además de la obligación legal, por supuesto.

Más dificultades se tiene, parece, a la hora de concretar el derecho. La obligación derivada del artículo 20 bis del ET y del 88 de la LOPDGDD, nos obliga a realizar algunas recomendaciones para poder influir en la política interna que el artículo 88 obliga a elaborar a la empresa previa audiencia a la RLT.

Requisitos de la Política Interna conforme al art. 88

- Tiene como objetivo garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.
- Su ejercicio debe acogerse a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y la RLT.
- Debe, en todo caso, atender a la naturaleza y objeto de la relación laboral y a la promoción del derecho a la conciliación de la actividad laboral y la vida personal y familiar.
- Debe culminar con la elaboración por la empresa, previa audiencia de la RLT, con una política interna dirigida a la plantilla, incluidos quienes ocupen puestos directivos, en la que se definan:
    - Modalidades de su ejercicio.
    - Acciones de formación y sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática.

[4] La AEPD publica recomendaciones en materia de Protección de Datos. Recientemente ha retirado la infografía "Privacidad y Seguridad en Internet" por no estar adaptado al nuevo Reglamento, pero es previsible que actualice la misma.

- En particular, se deberá preservar el derecho en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado/a vinculado al uso con fines laborales de herramientas tecnológicas.

Recomendaciones

Aunque habrá ocasión de profundizar más en esta materia, podemos adelantar algunas recomendaciones para afrontar nuestra participación en la elaboración de la política interna o en la negociación del convenio colectivo.

- El artículo 88, requiere un conocimiento en profundidad de las condiciones de trabajo de todas las personas de la plantilla: tipo de contrato, utilización de dispositivos digitales, tiempo de exposición a los mismos, acuerdos en materia de teletrabajo, etc. Por tanto, se debe garantizar el acceso a esta información por parte de la RLT.
- Esta política no debe modificar ningún otro derecho reconocido legal o convencionalmente. Por ejemplo, no debe suponer un incremento de la jornada laboral, ni una modificación en el horario, ni la ampliación de horas extraordinarias o la obligatoriedad de las mismas o una redefinición de lo que son o no horas extraordinarias.
- El tiempo que exceda la jornada laboral establecida deberá tener la consideración de hora extraordinaria. Cada vez es más habitual ver documentos que consideran que el hecho de prolongar la jornada para finalizar un trabajo que no es derivado de una orden directa no se debe considerar como hora extraordinaria, por lo que deberemos evitar estas apreciaciones de las empresas.
- La formación y sensibilización en esta materia deberán realizarse en horario laboral.
- Se deberán establecer mecanismos que permitan desconectar los servidores en caso de teletrabajo y mecanismos de alertas que avise a la persona trabajadora de que ha excedido su jornada laboral o que se ha conectado fuera de ella, si es necesaria su conexión y así se ha acordado.
- Se puede acordar la ausencia de mensajería durante las reuniones de trabajo, que no se deberán prolongar fuera de la jornada de trabajo.
- El sistema de registro de jornada tiene que servir para garantizar este derecho a la desconexión y ser capaz de registrar cualquier conexión fuera del horario laboral.
- El teletrabajo debe estar acordado entre empresa y RLT para evitar perjuicios en los derechos y salud de las personas que teletrabajan.
- Donde sea posible, instaurar una política de "luces apagadas" puede contribuir a hacer efectivo este derecho.
- Las circunstancias especiales de determinados puestos de trabajo, se deben tratar como excepcionales, pero también deben estar sometidas a la regulación en materia de registro de jornada o derecho a la desconexión digital.
- La mejora de los derechos de conciliación y corresponsabilidad recogidos en el convenio colectivo favorece también el ejercicio de este derecho.

Sistemas de videovigilancia y grabación de sonidos en el lugar de trabajo

Es posible que las empresas traten las imágenes obtenidas a través de cámaras o videocámaras para el ejercicio de las funciones de control previstas en el art. 20.3 del Estatuto, con 2 condiciones:

- Que estas funciones se ejerzan dentro de un marco legal
- Y con los límites inherentes a ese marco.
- Que se informe con carácter previo, y de forma expresa, clara y concisa a las personas trabajadoras, y, en su caso, a su RLT acerca de esta medida.

No será necesario el deber de información:

- Si se hubiera captado la comisión flagrante de un acto ilícito por los trabajadores o trabajadoras y
- existiese el dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos de los artículos 15 a 22 del Reglamento, al que se refiere el 22.4 de la LOPDGDD. También podrá incluirse en el dispositivo informativo un código o conexión o dirección de internet a esta información.

No se admitirá la instalación de sonidos ni sistema de vigilancia, en ningún caso:

- En los lugares destinados al descanso o esparcimiento: aseos, vestuarios, comedores y análogos.

Los sistemas de grabación de sonido, sólo se admitirá:

- Cuando resulte relevantes los riesgos para la seguridad de las instalaciones, bienes y personas
- Derivados de la actividad que se desarrolle en el centro de trabajo
- Siempre bajo el principio de proporcionalidad, intervención mínima y con las garantías previstas anteriormente.
- Los sonidos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten con la integridad de las personas, bienes o instalaciones. En tal caso, igual que las imágenes, deberán ser puestas a disposición de la autoridad competente en el plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación. En este caso no será obligatorio el bloqueo del artículo 32.

Debemos insistir en la importancia de la aplicación del **principio de proporcionalidad** y el **derecho de información** lo que en todo caso se deberá reforzar en la negociación colectiva.

La jurisprudencia no admite la instalación generalizada de medios de captación de imagen o voz de los trabajadores/as cuando existen suficientes medios de control de la actividad laboral, pero sí la admite en circunstancias muy concretas en la que se entienda idónea, necesaria y proporcionada una medida de control de ese tipo (STC 39/2016)

En algún caso se ha estimado la vulneración del derecho a la protección de datos por la utilización de la empresa de grabaciones de imágenes obtenidas por cámara de videovigilancia instaladas como medida de seguridad pública en un lugar abierto al público para el control de la actividad laboral, sin haber informado previamente a los trabajadores y trabajadoras sobre la finalidad a la que podían ser destinadas, derecho que no puede ser suplido o subsanado por la existencia de anuncios sobre la instalación de cámaras o por que se hubiera notificado la creación del fichero a la AEPD (STC 20/2013)

La primera sentencia que se dictó en España sobre la validez de una prueba de videovigilancia tras la aprobación de la LOPD (SJS nº 3 de

Pamplona, de 18-2-19) declara la nulidad de la prueba aportada por la empresa. Hasta ahora se consideraba suficiente para el cumplimiento del deber de información la mera exposición en un lugar visible del cartel distintivo, sin embargo, tras el Reglamento y las sentencias dictadas por el TEDH, debe concretarse por la empresa que las grabaciones pueden usarse con una finalidad sancionadora, lo que debe hacerse en el momento de instalarse las cámaras y una vez se contrate al trabajador/a. Recuerda la referencia a la información "previa, expresa, clara y concisa" y al Reglamento que es muy claro en materia de información y transparencia.

Vale para este caso también, algunas de las recomendaciones realizadas en los casos anteriores. La jurisprudencia y recomendaciones en esta materia han sido abundantes, e incluso la AEPD ha publicado una guía [5]sobre los sistemas de videovigilancia, aunque no hace referencia expresa al ámbito laboral, por lo que nos hace pensar que desarrollará próximamente esta materia.

Sistemas de geolocalización

¿Qué son los sistemas de geolocalización?

Son aquellos que permiten obtener datos de localización de la persona trabajadora. Es decir, es cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de una persona usuaria de un servicio de comunicaciones electrónicas disponible para el público.

Los datos de localización son por tanto datos personales, ya que se refieren siempre a una persona física identificada e identificable y se le aplica la normativa prevista para protección de datos.

Límites a la utilización de sistemas de geolocalización de la empresa

- Que la finalidad de su utilización sea la del ejercicio de sus funciones de control previstas en el artículo 20.3 del Estatuto. Por ejemplo, sería justificable el tratamiento de estos datos en defensa del interés legítimo de la empresa en localizar sus vehículos o cuando sean necesarios para mantener o cumplir el contrato de la relación laboral.
- Que estas funciones cumplan con las limitaciones y normas establecidas por la ley y con sus límites. Por ejemplo, no excluye el cumplimiento del deber de inscripción del correspondiente fichero y debe respetar los derechos de la persona trabajadora y el principio de proporcionalidad.
- La empresa debe informar de forma expresa, clara e inequívoca a las personas trabajadoras y su RLT acerca de la existencia y característica de estos dispositivos y del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión. Debe evaluarse primero si el tratamiento para los fines es necesario y si la aplicación efectiva cumple los principios de proporcionalidad y subsidiaridad. Por ejemplo, si se permite el uso privado de un vehículo corporativo, la persona trabajadora deberá poder desactivar las medidas de monitorización.

Cómo debe ser esa información

El GT29 sugiere que preferiblemente dicha información sea exhibida en cada coche, a la vista del conductor/a.

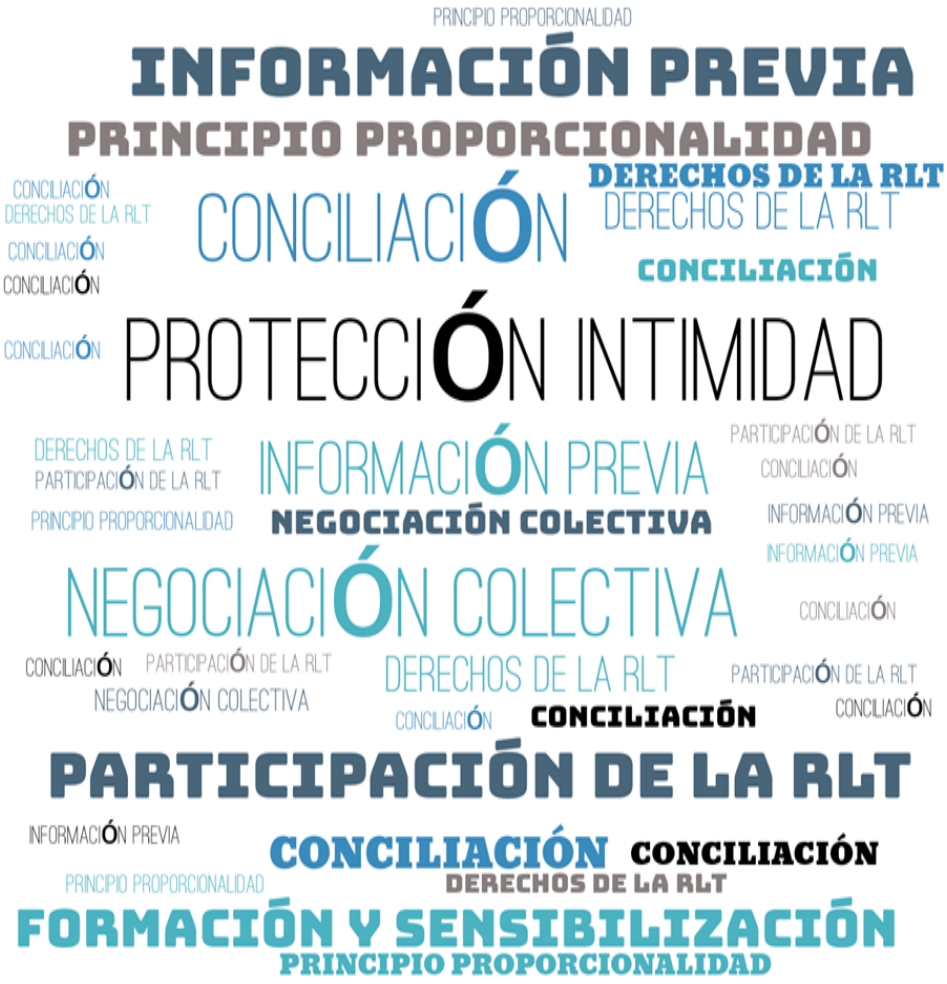
[5] Se puede consultar en https://www.aepd.es/media/guias/guia-videovigilancia.pdf.

En cuanto a la información sobre la medida, esta debería contener los siguientes aspectos:

- √ Su existencia.
- √ Cuándo se implantará y que permite obtener información durante la jornada laboral.
- √ Los derechos de acceso, rectificación y cancelación.
- √ Que estos datos formarán parte del Fichero de Personal de la empresa para gestionar la relación laboral existente.
- √ Si se van a ceder o no los datos a terceros.

> ***Recordemos que los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionadas con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral***

Será conveniente, por tanto, negociar con la empresa todas las cuestiones relacionadas con este asunto con antelación a su implantación, reforzando los principios de transparencia y proporcionalidad o salvaguardas específicas, por ejemplo estableciendo la prohibición de la geolocalización de las personas trabajadoras, también, en el ejercicio de su actividad sindical.



Respuestas a las preguntas recogidas en la página 12

¿Pueden contener datos de salud los justificantes de ausencia laboral?

El Reglamento General de Protección de Datos introduce en su artículo 5 los principios que deben respetarse en relación con el tratamiento de los datos personales. Uno de estos principios es el relativo a la minimización de datos.
Asimismo, no existe ninguna ley que habilite al empresario/a a tratar los datos de salud de las personas trabajadoras o familiares de los mismos. Por tanto, únicamente con el consentimiento explícito de los afectados podrían tratarse estos datos de salud.
Cabe indicar que no tendrá la consideración de dato de salud el hecho de que el justificante señale que la ausencia laboral se debe a una hospitalización o a una intervención quirúrgica sin hospitalización

Acceso del comité de empresa a un listado de las personas trabajadoras beneficiarias de la acción social.

Esta cesión únicamente podría entenderse amparada en caso de que se produjera *en el ámbito de las funciones desarrolladas por los Delegados de Personal o el Comité de Empresa* (según sea uno u otro al órgano de representación de los trabajadores), al encontrarse reconocido por el Estatuto de los Trabajadores el derecho de los representantes de los trabajadores, principalmente en el artículo 64, a acceder a determinados datos de los trabajadores en el ámbito de sus competencias. En este sentido, el artículo 64. 7 b) del Estatuto de los Trabajadores remite al Convenio Colectivo la determinación de la participación de los representantes de los trabajadores en la gestión o tramitación de la ayuda social de la empresa.

Para la AEPD, la función de vigilancia y control, desde la perspectiva de la protección de datos de carácter personal, podría entenderse correctamente cumplida sin necesidad de proceder a una información masiva.

Sólo en el supuesto en que la vigilancia o control se refieran a un *sujeto concreto*, que haya planteado la correspondiente queja ante el Comité de Empresa, será posible la cesión de datos específicos de dicha persona. En los demás supuestos, la función de control quedará plenamente satisfecha, a nuestro juicio, mediante la cesión de la información debidamente disociada, que permita al Comité conocer las circunstancias cuya vigilancia le ha sido encomendada sin referenciar la información en un sujeto concreto.

En consecuencia, procederá, en caso de haber sido formalmente solicitada, la cesión de los datos de las ayudas concedidas, siempre que los mismos sean cedidos de forma disociada, *sin poder referenciar los datos a personas identificadas o identificables*. En caso contrario, deberá recabarse el consentimiento de los interesados.

Las tarjetas identificativas de los trabajadores ¿Pueden incluir nombre, apellidos y DNI?

Estos trabajadores, que deben llevar dichas tarjetas identificativas, están de cara al público y en consecuencia, sus datos estarán a la vista de terceras personas ajenas al estricto ámbito laboral. Si la finalidad que justifica la inclusión de los datos de identidad de los trabajadores en sus tarjetas es precisamente garantizar su identificabilidad en el desempeño de sus funciones, el tratamiento de los datos puede considerarse amparado en el marco de la ejecución de un contrato, en base a lo dispuesto en el artículo 6 del RGPD, y sin perjuicio del cumplimiento del derecho de información del artículo 13 de la misma norma.

Vulnera la normativa de protección de datos utilizar un sistema de fichaje usando en la

aplicación de una función numérica a cada empleado fundada en un algoritmo generado por su huella digital?

El tratamiento de la huella digital para el control de cumplimiento de la jornada laboral ha sido indirectamente considerada por la Audiencia Nacional en sentencia de 4 de marzo de 2010, considerando que en este caso no sería preciso contar con el consentimiento de los trabajadores, sin perjuicio del ineludible cumplimiento por parte del empresario del derecho de información.

En el presente caso, se indica que los sistemas no incorporarán el dato de la huella digital sino únicamente el relacionado con un identificador numérico obtenido a partir de la misma que se almacena en las tarjetas de proximidad de los empleados.

De este modo, en el momento de acceso al edificio se utilizarán por el empleado terminales en los que será necesario tanto la aproximación de la tarjeta como la lectura de la huella digital. 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.

¿Pueden cederse los datos de salarios y TC2 de una subcontrata a la empresa principal?

Puesto que el TC2 contiene datos de salud y en las nóminas pueden aparecer datos relativos a la afiliación sindical, no son de aplicación las causas legitimadoras del artículo 6 del RGPD sino lo regulado en su artículo 9.

Respecto a la cesión del TC2, el artículo 42.2 del Estatuto de los Trabajadores, impone al contratista principal una responsabilidad solidaria, responsabilidad que implica atender el cumplimiento de una obligación de naturaleza salarial y las referidas a la Seguridad Social durante el período de vigencia de la contrata.

Además el propio Código Civil exige atender íntegramente las obligaciones solidarias por lo que es preciso conocer el contenido de la misma.

En consecuencia, la cesión de los TC2 estaría amparada en el artículo 9.2.b) -tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de los derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y seguridad y protección social-, en relación con el artículo 42.2 del Estatuto de los Trabajadores y por el alcance que el Código Civil impone a las obligaciones solidarias.

En cuanto a la comunicación de las nóminas, como regla general, el dato de la afiliación sindical tiene la naturaleza de categorías especial de datos. El tratamiento del dato relativo a la afiliación sindical se efectúa por el empresario, para que de la nómina se detraiga la cuota sindical correspondiente. Dado que la finalidad de dicho tratamiento va ligada al pago de la nómina y que en virtud de la obligación solidaria que impone el artículo 42.2 del Estatuto de los Trabajadores, al contratista principal, podemos concluir que el tratamiento de dicha información es para un fin idéntico del que justifica el tratamiento efectuado por el subcontratista. Por ello, siendo los fines idénticos, podemos entender que la comunicación de dichos datos es conforme, teniendo en cuenta también obligación impuesta por el artículo 42.2 del Estatuto de los Trabajadores.

En todo caso, el acceso por parte del contratista debería limitarse a los datos relacionados con los trabajadores subcontratados y no a cualesquiera trabajadores de la empresa subcontratada.

¿Se puede instalar GPS en los coches de empresa que utilizan los trabajadores?

La legitimación que permitiría este tratamiento de datos personales sería, en base a lo dispuesto en el artículo 6 del RGPD, la ejecución de un contrato, teniendo en cuenta, además, que el artículo 20.3 del Estatuto de los Trabajadores establece que el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

No obstante, la existencia de esta legitimación, sin necesidad de que preste consentimiento previo el trabajador, no excluye el cumplimiento del derecho de información del artículo 13 del RGPD. De esta forma, con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

¿Puede solicitar el empresario el teléfono y dirección de correo electrónico particular del trabajador?

El tratamiento del dato del correo electrónico y teléfono particulares del trabajador puede ser ignorado por el empresario, dado que ninguna norma exige que el trabajador, para la adecuada perfección de su relación contractual, haya de facilitar estos datos al empresario al que presta sus servicios.

Es decir, dicho tratamiento excedería en cuanto al mismo de lo permitido inicialmente por la normativa de protección de datos, y más concretamente, de la legitimación del artículo 6 del RGPD en base a la ejecución de un contrato. No obstante, si las circunstancias de la prestación de servicios para la empresa conllevara una disponibilidad personal del trabajador fuera de su centro u horario de trabajo, una medida más moderada e igual de eficaz para conseguir la comunicación de la empresa con el trabajador sería la puesta a disposición del mismo de un instrumento de trabajo como sería un teléfono de empresa.

En todo caso, sería posible que los afectados facilitaran los datos referentes a su e-mail y número telefónico particulares, si bien la recogida de estos datos habría de ser de cumplimentación voluntaria, previa la obtención del consentimiento del trabajador, que podrá oponerse posteriormente a su tratamiento ejerciendo los derechos de oposición o supresión.

¿Se pueden solicitar los antecedentes penales para un puesto de trabajo?

La LOPDGDD establece en su artículo 10 que los datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en la propia LOPDGDD o en otras normas de rango legal.

Por consiguiente, no es legalmente posible exigir a los candidatos 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 específicas normativas 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 LOPDGDD la solicitud de un certificado de antecedentes penales a las personas que se contraten por una entidad en el supuesto de que una Ley nacional, o una norma europea de directa aplicación, contemplen dicha medida, en otro caso, la misma resultaría contraria a lo regulado en la normativa de protección de datos.

¿Es factible comunicar los resultados de reconocimientos médicos al empresario, comité de empresa y sección sindical?

En lo que se refiere al tratamiento de los datos de salud por los servicios de prevención según el artículo 22.1 de la Ley 31/1995, 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.

Si bien es voluntaria para el trabajador, de este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad". Asimismo, y según el apartado 3 del citado artículo 22, "Los resultados de la vigilancia a que se refiere el apartado anterior serán comunicados a los trabajadores afectados".

Por último el párrafo segundo del artículo 22.4 de la Ley 31/1995 establece que "El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador", añadiendo el párrafo tercero que "No obstante lo anterior, el empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva".

En consecuencia, el empresario y los órganos con responsabilidades en materia de prevención, sólo podrán acceder a las conclusiones de dicha vigilancia de la salud referidas al concepto de "apto o no apto", salvo consentimiento expreso del trabajador**.**

¿Es necesario el consentimiento del trabajador para implantar un sistema de control horario? ¿Hay que informarle acerca de las medidas de control establecidas?

Con carácter general y para la implementación del registro de jornada no se precisa el consentimiento del trabajador, siendo base suficiente de legitimación la propia norma laboral, que en el artículo 34.9 ET establece la obligación de las empresas de realizar dicho registro de la jornada con carácter individual de cada persona trabajadora y que, de acuerdo con lo previsto en el artículo 6.1.c del Reglamento europeo 2016/679 (RGPD), el tratamiento de datos personales de los trabajadores derivado de la implantación del registro de jornada es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. No obstante lo anterior, la existencia de una lícita condición para el tratamiento de los datos de los empleados sin necesidad del consentimiento de los trabajadores no excluye el deber de las empresas de informar a los trabajadores de la existencia del registro y de la finalidad del tratamiento de los datos personales individuales que se obtienen con dicho registro.

En el caso de que se trabaje con proveedores, ¿Cómo se establece esa relación para el

control horario?

Las empresas que sean empleadores, con relación a sus trabajadores, actuarán como responsables del tratamiento de los datos obtenidos mientras que, en su caso, los proveedores externos de los sistemas de registro actuarán como entidades encargados del tratamiento, con las obligaciones que respectivamente para entidades responsables o entidades encargadas dispone la normativa de protección de datos. Para ello se deberá suscribir el correspondiente contrato de encargo con el contenido que contempla el art. 28 RGPD.

¿Puede solicitar el empresario el teléfono y dirección de correo electrónico particular del trabajador?

El tratamiento del dato del correo electrónico y teléfono particulares del trabajador puede ser ignorado por el empresario, dado que ninguna norma exige que el trabajador, para la adecuada perfección de su relación contractual, haya de facilitar estos datos al empresario al que presta sus servicios.

Es decir, dicho tratamiento excedería en cuanto al mismo de lo permitido inicialmente por la normativa de protección de datos, y más concretamente, de la legitimación del artículo 6 del RGPD en base a la ejecución de un contrato. No obstante, si las circunstancias de la prestación de servicios para la empresa conllevara una disponibilidad personal del trabajador fuera de su centro u horario de trabajo, una medida más moderada e igual de eficaz para conseguir la comunicación de la empresa con el trabajador sería la puesta a disposición del mismo de un instrumento de trabajo como sería un teléfono de empresa.

En todo caso, sería posible que los afectados facilitaran los datos referentes a su e-mail y número telefónico particulares, si bien la recogida de estos datos habría de ser de cumplimentación voluntaria, previa la obtención del consentimiento del trabajador, que podrá oponerse posteriormente a su tratamiento ejerciendo los derechos de oposición o supresión.

Fuentes consultadas y de interés para ampliar información

Páginas web

Agencia Española de Protección de Datos

CCOO

CCOO de Industria

Regulación y normativa

Normativa protección de datos de carácter personal

Guías de trabajo del artículo 29:

Guía del Grupo de trabajo del artículo 29 sobre transparencia en el Reglamento 2016/679

Guía del Grupo de trabajo del artículo 29 sobre el consentimiento en el Reglamento 2016/679

Guía del Grupo de trabajo del artículo 29 sobre el derecho a la portabilidad

Preguntas frecuentes

Guía del Grupo de trabajo del artículo 29 sobre el delegado de protección de datos (DPD)

Preguntas frecuentes

Guía del Grupo de trabajo del artículo 29 para identificar a la autoridad de control líder

Preguntas frecuentes

Guía del Grupo de trabajo del artículo 29 para la evaluación del impacto en la protección de datos (DPIA) y para determinar si un tratamiento puede generar un alto riesgo a los efectos del Reglamento 2016/679

Guía sobre la notificación de las violaciones de seguridad

Guía sobre decisiones automatizadas y la elaboración de perfiles

Guía sobre la aplicación y la determinación de las multas administrativas

Otra información de interés

Lefebvre. Base de Datos. Memento social. Parte III Protección de datos.

Editorial Aranzadi. Los Derechos Digitales de las personas trabajadoras. Carlos Hugo Preciado Domenech.

Editorial Bomarzo. El derecho del trabajo y los retos planteados por la globalización y digitalización de la economía. Manuel Correa Carrasco.

Editorial Bomarzo. Protección de datos personales del trabajador en el proceso de contratación: facultades y límites de la actuación del empleador. Jesús Cruz Villalón.

Editorial Bomarzo. La protección de datos y la regulación de las tecnologías en la negociación colectiva y la Jurisprudencia. Juana María Serrano García.

Resoluciones Judiciales relativos a los derechos individuales de las personas trabajadoras

Control por la empresa de los dispositivos digitales utilizados por las personas trabajadoras.

Tribunal Europeo de Derechos Humanos

– STEDH de 5 de septiembre de 2017, caso Barbulescu.

Hay violación del artículo 8 CEDH (Convenio de protección de derechos y libertades fundamentales) **por parte de la empresa porque, aunque el empleador había puesto en conocimiento del trabajador la prohibición del uso de medios informáticos e internet en la empresa para usos personales, ni le había advertido con carácter previo de que iba a someterle a vigilancia, ni del alcance ni naturaleza de tal vigilancia.**

– STEDH de 22 de febrero de 2018, caso Libert.

El Tribunal considera que no existe una violación de la vida privada en un supuesto de despido de un trabajador, tras la incautación de su ordenador profesional, que reveló el almacenamiento de ficheros de carácter pornográfico y certificaciones falsas libradas en favor de terceros. Constata que la consulta de los ficheros por el empresario respondió a un objetivo legítimo, cual es el de asegurarse que los trabajadores utilizan adecuadamente los equipos informáticos puestos a su disposición.

Tribunal Constitucional

– STC 170/2013, de 7 de octubre.

Basta que un convenio colectivo sancione la utilización de herramientas informáticas y correo electrónico para usos diversos al profesional, para considerar que la empresa puede controlar los correos electrónicos de los empleados sin aviso previo a los mismos y sin que ello vulnere su derecho al secreto de las comunicaciones y el derecho a la intimidad.

– STC 170/2011, de 7 de noviembre.

En el marco de las facultades de autoorganización, dirección y control correspondiente a la empresa, es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización de los medios en cuestión.

Tribunal Supremo

– STS, social, de 8 de febrero de 2018, rec. 1121/2015.

Control del correo electrónico del trabajador. Se declara procedente el despido por haber incurrido en transgresión de la buena fe contractual y abuso de confianza, al haber aceptado de otra empresa dos transferencias bancarias por importe de 11.000 y

39.000 euros, considerando que el control del correo electrónico del trabajador fue una prueba lícita.

Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo

Tribunal Europeo de Derechos Humanos

– STEDH 9 de enero de 2018, caso López Ribalda contra España.

El empresario instaló cámaras visibles, de las que informó al personal, y otras cámaras ocultas, que enfocaban a las cajas y de las que no informó, por lo que los trabajadores no supieron nunca que eran filmados en las cajas. Estas últimas cámaras grabaron a las trabajadoras mientras ayudaban a clientes y a otras compañeras a sustraer artículos, llevando a cabo también ellas mismas algunas sustracciones. Los órganos judiciales españoles declararon la procedencia del despido. El TEDH considera que la videovigilancia oculta de un trabajador en su puesto de trabajo es una injerencia en su derecho a la vida privada. Si bien la prueba es ilícita, y por tanto, nula, existen pruebas lícitas desconectadas por la anterior que permiten declarar el despido procedente.

– STEDH 28 de noviembre de 2017.

La instalación de un sistema de videovigilancia en los lugares de enseñanza (aulas universitarias) constituye una injerencia en el ejercicio por los demandantes de su derecho a la vida privada, y ello aunque la zona de videovigilancia fuera un lugar público de trabajo.

– STEDH 5 de octubre de 2010.

La grabación de un trabajador en su puesto de trabajo debe ser considerada como una intromisión en su vida privada.

Tribunal Constitucional

– STC 37/1998, de 17 de febrero.

Se declara el carácter desproporcionado de la filmación por agentes de policía de un piquete de huelga, por ser disuasoria del ejercicio de los derechos de huelga y libertad sindical.

– STC 98/2000, de 10 de abril.

La instalación de un sistema de grabación y captación de sonidos en un casino, que permite la audición continuada e indiscriminada de todo tipo de conversaciones, tanto de los trabajadores como de los clientes, constituye una actuación que rebasa las facultades que otorga al empresario el artículo 20.3 ET y supone una intromisión ilegítima en el derecho a la intimidad.

– STC 186/2000, de 10 de junio.

Se declara proporcionada la videovigilancia no advertida ni al comité de empresa ni a los trabajadores afectados, ya que previamente se habían advertido irregularidades en el comportamiento de los cajeros de determinada sección del economato y un acusado

descuadre contable. Considera que la medida fue proporcionada, al existir razonables sospechas de actuación irregular por parte de los trabajadores, que justificaban el control oculto.

– STC 29/2013, de 11 de febrero.

El TC considera nula la prueba de captación de imágenes del trabajador en lugares públicos de paso a fin de controlar su actividad laboral, porque ni el trabajador mismo ni el comité de empresa habían sido informados del establecimiento de un sistema de control de la actividad laboral.

– STC 39/2016, de 3 de marzo.

El TC considera que el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, al tratarse de una medida dirigida a controlar el cumplimiento de las obligaciones derivadas de la relación laboral.

2.2.3. Tribunal Supremo

– STS 13 de mayo de 2014, rec. 1685/2013.

Se declara el despido nulo, al basarse en grabaciones con cámaras destinadas a otra finalidad distinta al control de la actividad laboral. En el caso la empresa no dio información previa a la trabajadora de la posibilidad de que fuera grabada ni de la finalidad de las cámaras instaladas. Tampoco se comunicó a la representación de los trabajadores.

– STS 7 de julio de 2016, rec. 3233/2014.

Contempla el caso de una empleada de supermercado que, junto con otra, consumía productos de la empresa en el almacén, constando como hecho probado que todo el personal tenía conocimiento de la instalación de cámaras de vigilancia, dando validez a la prueba así obtenida.

– STS 31 de enero de 2017, rec. 3331/2015.

Validez de las pruebas de videovigilancia empleadas por la empresa para justificar el despido de un trabajador, que era conocedor de la existencia de dicho sistema de grabación aunque no fuera informado del destino que pudiera darse a las imágenes obtenidas.

– STS 1 de febrero de 2017, rec. 3252/2015.

Validez de las imágenes obtenidas mediante cámaras de seguridad, en un caso en el que la trabajadora conocía la existencia de dichas cámaras, aunque no fuera informada del destino que pudiera darse a las imágenes.

Tribunal Superior de Justicia

– STSJ Madrid de 25 de enero de 2019, rec. 971/2018.

Despido procedente. No se ha vulnerado el derecho a la intimidad, ya que la instalación de cámaras es una medida justificada e idónea, conociendo los trabajadores su existencia, uso y destino. Prueba lícita. En igual sentido SSTSJ Andalucía/Granada de 10

de octubre de 2018, rec. 2260/2017; Castilla y León/Burgos de 22 de junio de 2017, rec. 384/2017 y Castilla-La Mancha de 14 de enero de 2016, rec. 1474/2015.

– STSJ Madrid de 28 de septiembre de 2018, rec. 275/2018.

Despido improcedente. Imágenes obtenidas mediante cámaras instaladas en la zona de acceso al centro de trabajo y que se utilizan también para el control de las obligaciones laborales. Prueba obtenida ilícitamente al no haber sido informado el trabajador, ni prestado su consentimiento. En los mismos términos Madrid de 13 de septiembre de 2018, rec. 417/2018.

– STSJ Madrid de 4 de junio de 2018, rec. 217/2018.

Despido improcedente. Vulneración del derecho a la intimidad del trabajador por la instalación de cámaras de viodevigilancia, incumpliendo la obligación de informar a al mismo.

– STSJ País Vasco de 27 de febrero de 2018, rec. 226/2018.

Despido nulo. Vulneración del derecho a la intimidad por la instalación de cámaras incumpliendo la empresa el deber de información al trabajador de la existencia del sistema de videovigilancia.

Utilización de sistemas de geolocalización en el ámbito laboral

Tribunal Europeo de Derechos Humanos

– STEDH 2 de septiembre de 2010.

Considera el Tribunal que la instalación de un sistema GPS constituye una injerencia en la vida privada de la persona.

Audiencia Nacional

– SAN 6 de febrero de 2009, procedimiento 318/2018.

Nulidad de la implantación de un GPS, para lo cual el trabajador, con categoría de repartidor, ha de aportar un teléfono y móvil de su propiedad con conexión a internet.

Tribunal Superior de Justicia

– STSJ Madrid de 12 de julio de 2019, rec. 197/2019.

Existe vulneración del derecho fundamental a la intimidad, por la instalación de GPS en el vehículo sin informar al trabajador ni al comité de empresa, reportando información durante las 24 horas del día. Condena a la empresa a la inmediata retirada del GPS y a abonar 12.000 euros en concepto de daños morales.

– STSJ Asturias de 27 de diciembre de 2017, rec. 2241/2017.

Existe vulneración de derechos fundamentales por el hecho de tener activado el GPS fuera de la jornada laboral, sin el imprescindible conocimiento de los trabajadores.

– STSJ Andalucía/Granada de 19 de octubre de 2017, rec. 1149/2017.

Despido nulo. Utilización de los datos del GPS instalado en el vehículo puesto a disposición del trabajador de manera permanente.

– STSJ Comunidad Valenciana de 2 de mayo de 2017, rec. 3689/2016.

No existe vulneración de derechos fundamentales cuando la instalación del GPS es conocida por el trabajador.

– STSJ Madrid de 29 de septiembre de 2014, rec. 993/2013.

Vulneración del derecho a la intimidad por colocación de GPS en el vehículo que permite conocer el lugar exacto en el que se halla, incluso fuera de la jornada. En los mismos términos Castilla-La Mancha de 10 de junio de 2014, rec. 1162/2013.

– STSJ Madrid de 21 de marzo de 2014, rec. 1952/2013.

Lesión del derecho a la intimidad por instalación del GPS en el vehículo cedido al trabajador para uso profesional, sin informarle de dicha circunstancia.

Derecho a la desconexión digital

Tribunal Constitucional

– STC 192/2003, de 27 de octubre.

Indirectamente se refiere a esta cuestión, ya que el procedimiento tenía por objeto una declaración judicial de procedencia del despido por realizar trabajos para otra empresa durante el periodo vacacional. Mantiene el TC que la concepción del periodo anual de vacaciones como tiempo cuyo sentido principal es la reposición de energías para la reanudación de la prestación laboral supone reducir la persona del trabajador a un mero factor de producción y negar, en la misma medida, su libertad, durante aquel periodo vacacional, para desplegar la propia personalidad del modo que estime más conveniente.

Tribunal Supremo

– STS 21 de septiembre de 2015, rec. 259/2014.

Se establece la nulidad de una cláusula tipo del contrato de trabajo en la que se hace constar la posibilidad de que la empresa pueda efectuar comunicaciones al trabajador vía SMS o vía correo electrónico, según los datos facilitados por el trabajador a efectos de contrato, con la obligación, además, de comunicar a la empresa de forma inmediata cualquier cambio o incidencia en el teléfono o en el correo electrónico.

Audiencia Nacional

– SAN 17 de julio de 1997, procedimiento 120/1997.

Enjuicia la validez de una orden de conexión de las trabajadoras, que les obligaba a mantener la escucha de los teléfonos móviles en horas no coincidentes con la jornada de trabajo. Se estima que tal obligación sobrepasa las facultades normales y regulares de la empresa, al obligar a los trabajadores a estar pendientes de recibir instrucciones en todo momento, incluso en horas no coincidentes con la jornada de trabajo.

Otros pronunciamientos judiciales de interés sindical

– SAN, contencioso, 21 de junio de 2019, rec. 667/2018.

Confirma la sanción de 5.000 euros impuesta a un sindicato, por hacer público en su tablón de anuncios la nómina de un trabajador en la que figuran sus datos personales y económicos, incluida su dirección particular.

– SAN, contencioso, 1 de enero de 2013.

Confirma la sanción de 3.000 euros a una empresa que facilitó a un sindicato, con motivo de las elecciones sindicales, las direcciones particulares de los trabajadores que integraban el censo de una mesa y a los que se remitió propaganda electoral. Inexistencia de consentimiento de los afectados para facilitar dicho información.

– SAN, contencioso, 4 de marzo de 2010, rec. 274/2009.

Confirma sanción de 6.000 euros a un sindicato por remitir propaganda electoral a domicilios particulares, sin contar con autorización de los destinatarios.

Sobre las materias anteriores existen numerosas resoluciones de la AEPD, algunas de ellas con bastante interés. Se pueden consultar en la web de la AEPD.

– Resolución de 12 de julio de 2019, procedimiento 112/2015. Sanción a una empresa por instalar un GPS en el móvil sin consentimiento ni información al trabajador.

– Resolución de 27 de diciembre de 2018, procedimiento 72/2018.

– Resolución de 27 de diciembre de 2018, AP 52/2018.

– Resolución de 14 de marzo de 2018, AP 75/2015.

– Resolución de 21 de julio de 2018, procedimiento 01731/2015.

– Resolución de 27 de diciembre de 2018, procedimiento 43/2018.

– Resolución de 20 de julio de 2017, procedimiento AP/55/2016.