PROTOCOLO DE ACTUACIÓN PARA LA NEGOCIACIÓN COLECTIVA

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y GARANTÍAS DE LOS DERECHOS DIGITALES

NORMATIVA APLICABLE 3

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) 7

LOS DICTÁMENES DEL GRUPO DE TRABAJO DEL ART. 29, ACTUAL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS 7

FINALIDAD DEL PROTOCOLO DE ACTUACIÓN PARA LA NEGOCIACIÓN COLECTIVA 7

LOS DATOS DE CARÁCTER PERSONAL, QUÉ DATOS LO SON Y CUÁLES NO 9

EL CONSENTIMIENTO DEL TRABAJADOR 19

LA GARANTÍA DE LOS DERECHOS DIGITALES 24

NORMATIVA APLICABLE

El Reglamento comunitario cuya aplicación directa comenzó el día 25 de mayo de 2018, REGLAMENTO 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE, determina la protección del derecho de las personas y ciudadanos de la UE, en cuanto a tales, y como trabajadores y trabajadoras, a la protección de sus datos de carácter personal, en todos los ámbitos de la vida, incluido el de las relaciones laborales.

El inicio del cambio legislativo fue la Comunicación titulada: "un enfoque global de la protección de los datos personales en la Unión Europea" (UE), de 4 de noviembre de 2010, que constituyó el germen de la posterior reforma del marco legal en materia de protección de datos.

Aunque la finalidad del Reglamento es garantizar la libre circulación de los datos en toda la UE, aumentando la claridad de la regulación, para que sea posible la transferencia de los mismos en el llamado "mercado único digital", también se reconoce que los representantes de los trabajadores y sindicatos, en la promoción y defensa de los derechos de los trabajadores, lleguen a los acuerdos que sean necesarios dentro de los convenios colectivos, desde el ámbito sectorial estatal, hasta el convenio de empresa, para proteger este derecho fundamental.[1]

La propia Organización Internacional del Trabajo (OIT), ya alertó de los peligros de vulneración de numerosos derechos en conflicto, en relación con la recogida de datos de carácter personal en las relaciones de trabajo y la influencia de la informática, sobre la posible invasión por la misma, de la privacidad de los trabajadores y trabajadoras y también la posible vulneración de los datos relativos al derecho de libertad sindical desde el punto de vista del derecho de afiliación y autoorganización de los sindicatos.

Así, en la reunión de expertos llevada a cabo en Ginebra durante la primera semana de octubre de 1996, sobre la protección de la vida privada de los trabajadores, y en cumplimiento de la Decisión tomada por el Consejo de Administración de dicha Organización se estableció un repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores, que en determinados postulados sigue vigente.[2]

Por otra parte, y en el ámbito del Consejo de Europa, el Convenio 108 plus, ha venido a ampliar los contenidos y la protección del Convenio 108, concluido en el

año 1981, con la finalidad de proteger a los ciudadanos respecto al tratamiento automatizado de los datos de carácter personal. La nueva versión, se firmó el 10 de octubre de 2018 en Estrasburgo, pasando a denominarse Convenio 108 (+) plus, siendo España uno de los países firmantes.[3]

En el ámbito de la regulación de los derechos humanos, se encuentra un instrumento fundamental en esta materia: el "Convenio para la protección de los derechos y de las libertades fundamentales"[4], regulando en el art. 8, el derecho al respeto de la vida privada y familiar: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia", habiendo dictado el Tribunal Europeo de Derechos Humanos (TEDH) importantes sentencias en relación con dicho derecho, como Barbulescu I, Barbulescu II, y López Ribalda, entre otras.

Nuestra Norma Fundamental en el art. 18.4, fue una de las primeras en limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, habiéndose dictado por parte del Tribunal Constitucional (TC), numerosas sentencias también en la materia, aunque el criterio interpretativo no ha sido ni unánime, ni se ha mantenido en el tiempo, sino que ha ido evolucionando. Criterio que deberá adecuarse a las sentencias europeas y a los nuevos principios legales y, en su caso, a los postulados convencionales que se vayan estableciendo negocialmente.[5]

La aplicación directa del Reglamento comunitario conlleva que, en caso de que entre en contradicción la Ley Orgánica, 3/2018, de 5 de diciembre, para la Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), con él, prime la regulación de dicho Reglamento, de la misma manera que primará la interpretación del Tribunal de Justicia de la Unión Europea (TJUE), respecto de la de nuestros tribunales internos, independientemente de que el TEDH también puede determinar cuál es la doctrina adecuada, cuando lo que se vulnera es el derecho humano a la vida privada.

El cambio de Gobierno del Partido Popular, provocó otro cambio, el de la tramitación del proyecto de ley de la norma mencionada en el párrafo anterior, y el Partido Socialista Obrero Español (PSOE), incorporó numerosas novedades al texto, en su mayoría pactadas con el PP y el resto de grupos políticos, por lo que el texto final del Proyecto se aprobó por unanimidad.

Como la propia norma excluye del ámbito de aplicación, los tratamientos que se rijan por disposiciones específicas, serán objeto de futuras, pero seguro que cercanas, regulaciones especiales, otras cuestiones relativas a la transformación

digital y la protección de datos de los trabajadores y trabajadoras y de los ciudadanos en general y, por lo tanto, nuevas normas irrumpirán en la protección y desarrollo de este derecho.

Especial relevancia tiene la inclusión en la Ley Orgánica del Título X (arts. 79 a 97) denominado "Garantía de los derechos digitales", a fin de "reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución". La propia Exposición de motivos señala que sería deseable una futura reforma de la Constitución, una actualización de nuestra Norma Fundamental a la era digital y, específicamente, elevando a rango constitucional una nueva generación de derechos digitales, pero por el momento, las prescripciones legales no dejan de poner de manifiesto, el haber perdido una auténtica oportunidad de establecer unas adecuadas garantías, y el concepto de determinados derechos que parece difuso.

Como el Reglamento 2016/679, en el artículo 88 determina que: "los Estados miembros podrán a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de los datos personales de los trabajadores en el ámbito laboral en particular a los siguientes efectos[6]:

- *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,*
- *incluso[7] medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales,*

serán en todas estas materias en las que los convenios colectivos podrán establecer regulaciones adecuadas para la protección del derecho de las personas trabajadoras, por supuesto, con especial atención a:

- la transparencia del tratamiento,

- 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 supervisión se entiende el control de los trabajadores),

- además de poder establecer consideraciones específicas en materia de derechos digitales.

Es por ello por lo que la UGT, recogiendo la opción comunitaria determinada en el Reglamento, considera necesario que, en estos aspectos, los convenios colectivos tengan un papel importante, tanto de carácter pedagógico, como formativo, como regulador de la protección necesaria del derecho de protección de los datos de carácter personal de los trabajadores y trabajadoras, y la garantía de determinados derechos digitales.

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)

Es necesario referenciar también que existe un importante repertorio de resoluciones e informes de la Agencia Española de Protección de datos, (AEPD), en relación a algunas cuestiones en materia de relaciones laborales, que pueden servir como cierta "jurisprudencia" elaborada por nuestra autoridad de control independiente, garantizando y tutelando el derecho fundamental en cuestión. Aunque algunas de estas resoluciones ponen de manifiesto que el derecho fundamental de protección de datos puede ceder ante otros derechos como por ejemplo, la libertad sindical.[8]

LOS DICTÁMENES DEL GRUPO DE TRABAJO DEL ART. 29, ACTUAL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS

También es necesario conocer los Dictámenes del Grupo de Trabajo del Artículo 29, como órgano europeo independiente, (ahora Comité Europeo de Protección de datos), sobre todo los relativos al consentimiento, al tratamiento de datos en el trabajo, y al concepto de datos personales,[9] y cuyos dictámenes será importante seguir conociendo.[10]

FINALIDAD DEL PROTOCOLO DE ACTUACIÓN PARA LA NEGOCIACIÓN COLECTIVA

Este primer Protocolo de actuación es para los negociadores de los convenios colectivos, desde todos los niveles de negociación, desde el nivel sectorial estatal, hasta el convenio de empresa, con el objeto de servir de orientación y base, para establecer en la negociación colectiva, las directrices necesarias que permitan, desde el conocimiento por los trabajadores del contenido del derecho, hasta la limitación de las conductas organizativas empresariales que puedan vulnerarlo, protocolo que se irá modificando en función de las necesidades que vayan siendo conocidas y que provengan, tanto desde el ámbito sectorial estatal, como del empresarial, o debido a las posibles conductas ilícitas que puedan ir constatándose, o en su caso, teniendo en cuenta la interpretación que del derecho hagan tanto los tribunales europeos como los nacionales.

LOS DATOS DE CARÁCTER PERSONAL, QUÉ DATOS LO SON Y CUÁLES NO

Datos personales que hacen a los trabajadores y trabajadoras identificados o identificables, directa o indirectamente

Cualquier dato[11], independientemente de los más evidentes como el nombre y los apellidos o el número de DNI, cualquier información numérica, alfabética, gráfica, fotográfica, acústica, el correo electrónico, la dirección IP de Internet, del ordenador y del smarthphone, la huella dactilar, el iris de los ojos, un tatuaje, o cualquier otra circunstancia material o inmaterial que la identifique, incluida la huella digital del uso de las nuevas tecnologías y la conjunción de dos o más datos que hagan a esa persona ser posiblemente conocida, pero también los datos relativos a la salud o los datos relativos a condenas e infracciones penales, son datos protegibles de carácter personal.

Los datos de localización, como la función GPS de un teléfono móvil, el identificador de una cookie, o el identificador de la publicidad del teléfono, también pueden ser una forma de identificar a una persona.

En general, una persona es "identificada" cuando dentro de un grupo se la distingue de los demás, y es identificable por la información que nos permita hacerlo

Trabajador o trabajadora identificado

Una persona es "identificada" cuando dentro de un grupo se la distingue de los demás.[12]

Y es "identificable" como ya hemos dicho, por la información que nos permita hacerlo. Estos otros datos de carácter indirecto pueden tener una "relación privilegiada y muy cercana con una determinada persona", por ejemplo, " la altura, el color del cabello, la ropa, etc., o una cualidad de la persona que no puede percibirse inmediatamente, como su profesión, el cargo que ocupa, su nombre, etc.", pero que en conjunción con alguna otra de las anteriores puede hacerlo posible.

También se puede identificar indirectamente a una persona por un número de teléfono, la matrícula de un coche, un número de Seguridad Social, un número de pasaporte, o por una combinación de criterios significativos (edad, empleo, domicilio, etc.) que hagan posible estrechar el grupo al que pertenece, y

finalmente señalarla, pudiendo depender del contexto de que se trate, por lo que a veces depende el ser identificable, de un caso concreto.

El Tribunal de Justicia de las Comunidades Europeas (STJCE), se ha pronunciado en ese sentido al considerar que: " la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento de datos de carácter personal. Un dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa".

Que determinados datos, circunstancias de lugar, tiempo o circunstancias tecnológicas, permitan hacer que una persona sea identificable hace que no se pueda llevar a cabo el tratamiento de esos datos sin un adecuado nivel de protección, teniendo en cuenta los principios del Reglamento, sobre todo el deber de información previa.

El Convenio 108 del Consejo de Europa, adopta una definición amplia para abarcar que una información pueda vincularse a una persona, y la reforma del mismo adoptándose el Convenio 108 plus, tuvo en cuenta que fuera posible incluir "toda información referente a una persona que la haga identificable".

En relación con la videovigilancia las imágenes son datos, aunque no detecten personas. Como la finalidad de la videovigilancia es, identificar a las personas que aparecen en las imágenes de vídeo en todos aquellos casos en los que esa identificación es considerada necesaria por el responsable del tratamiento, hay que considerar el uso del sistema en sí, como tratamiento de datos sobre personas identificables, aun cuando algunas de las personas filmadas, insistimos, no sean identificables en la práctica.[13]

Las direcciones IP, también son consideradas datos de carácter personal, porque pueden hacer que una persona sea identificable. En este sentido, el Grupo de trabajo del art. 29, ha declarado que los proveedores de acceso a Internet y los administrados de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Y sobre todo, cuando el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador.

Datos que no hacen a un trabajador o trabajadora identificable

Hay datos indirectos que, pueden hacer a una persona identificable, pero también hay otros datos que no lo consiguen. La mera posibilidad de que con determinados datos se pueda identificar a alguien no es suficiente para hacer a una persona identificable.

Determinada información hace que algunos datos no sean de carácter personal,[14] si teniendo en cuenta el conjunto de los medios que pueden ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, no existe esa posibilidad o es insignificante.

Pero hay que tener en cuenta que los avances tecnológicos pueden hacer que unos datos no nos digan algo hoy y sí puedan decírnoslo en un futuro próximo.

Datos que por ejemplo, no son personales son: un número de registro mercantil, la dirección de correo electrónico del tipo: info@empresa.com, datos anonimizados (tachados, inventados, que sustituyen a los reales), etc.

Hay casos de dirección IP que no puedan identificar a una persona, si diversas razones técnicas y organizativas no permiten la identificación del usuario, por ejemplo, un ordenador instalado en un sitio público o de uso común por un número indeterminado de personas, porque no permite la identificación del usuario con medios razonables.

Algunos ejemplos de cómo puede ser identificable una persona[15]

Como ya hemos señalado, determinada información "sobre" una persona, puede hacerla identificable, por ejemplo:

- **los datos incluidos en el fichero personal** de alguien, guardados en el departamento de personal de una empresa, por estar claramente relacionados con su situación como empleado de dicha empresa,
- **los datos sobre los resultados de las pruebas médicas** a las que se ha sometido alguien, recogidos en su historial médico,
- **las imágenes filmadas** en video de una persona, en una entrevista,
- **si la información en lugar de a una persona se refiere a un objeto**, las normas sobre protección de datos no se aplicarán cuando esa información se utilice únicamente para ilustrar, por ejemplo, el nivel de precios de la

vivienda en una determinada zona. Sin embargo, si se dan determinadas circunstancias, esa información también debe considerarse como un dato personal, por ejemplo, a la hora de calcular los impuestos que deberá pagar un propietario. En este contexto, "tal información debe considerase como un dato de carácter personal",

- **cuando los datos se refieren a procesos o hechos**, por ejemplo, a la revisión del funcionamiento de una máquina, como el cuaderno en el que un mecánico o un garaje anotan las revisiones pasadas por un automóvil, contiene información sobre el mismo: kilometraje, fechas de las revisiones, problemas técnicos y estado de conservación, si la información se asocia en el cuaderno a una matrícula y a un número de motor que, a su vez, pueden vincularse con el mecánico que trabajó en el coche, esa información es de carácter personal,

- **el registro de llamadas de una línea de teléfono** proporciona información sobre las llamadas realizadas y sobre las recibidas, en estos casos, el concepto de datos personales abarca tanto las llamadas salientes como las entrantes, en la medida en que todas ellas contienen información sobre la vida privada, las relaciones sociales o las comunicaciones de las personas,

- **en las Actas de reunión, también hay datos de carácter personal y datos que no tienen ese carácter**, por ejemplo, en las reuniones hay multitud de personas intervinientes, y datos relativos algunas veces a unas y otras veces no se centran en ninguna persona, en estos casos es necesario analizar los datos en función de las características de los mismos. Por ejemplo, solo son datos personales que "PEPE" asista a una determinada reunión en un determinado lugar y haga determinadas declaraciones, pero el relato de los debates de "Juan" también en la reunión y sus declaraciones reflejadas en el acta por un tercero, no son datos personales sobre "PEPE", aunque sea "PEPE" el que sacó a relucir el tema sobre el que se debatió en la reunión, por lo que "PEPE" no podría acceder a cancelar dichos datos al no considerase de carácter personal propios",

- otros datos de carácter personal como incluir el nombre del trabajador o trabajadora que ha atendido a un determinado cliente en un comercio, **en el ticket de venta del comercio, y ticket que se pone a disposición del cliente** y que hace a esa persona identificada o identificable, sí es de carácter personal y si no se aplican los principios y prevenciones del Reglamento y de la LOPDGDD, sería ilícito hacerlo,[16]

- **el DNI electrónico tiene datos biométricos**, por lo que no debe utilizarse como método de control de los trabajadores. El art. 87 del RGPD establece que: "los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento". La disposición adicional séptima de la LOPDGDD, determina en relación con el DNI, que:

- en relación con la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

    - cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

    - si son anuncios, en los supuestos del artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

    - cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente,

- **Los datos estadísticos son datos personales en ocasiones**.

El INE, en una primera fase de su labor estadística guarda en forma no agregada información relativa a personas concretas, personas a las que se asigna un código en vez de un nombre, y se guardan por separado las claves de estos datos.

Cabe dentro de lo razonable, que el INE utilice esa clave, pero al conjunto de datos referentes a una persona concreta deben considerarse datos personales.

Sobre este particular ya ha resuelto la AEPD aunque en relación a la legislación anterior, pero la resolución sigue estando vigente. Dicho organismo ha señalado que: en el caso de cesión de los datos de los trabajadores, la misma 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, al encontrarse reconocido por el Estatuto de los Trabajadores (ET) el derecho de tales representantes, a acceder a determinados datos en el ámbito de sus competencias. Pudiendo tener cabida en el convenio colectivo regulaciones sobre este aspecto,[18]

- **a las personas jurídicas no se les protegen los datos**, no en el sentido de la regulación del Reglamento ni de la LOPDGDD, pero sí en el sentido de la protección de las comunicaciones electrónicas.

Obligaciones de la empresa

A) Obligación de aplicar medidas oportunas y eficaces para la protección de los datos:

Es necesario tener en cuenta que, el responsable del tratamiento de datos de carácter personal, está obligado a aplicar medidas oportunas y eficaces para la protección de los datos de carácter personal que se recaben, de cualquier tipo, y siempre que se puedan recabar, porque de lo contrario la recogida y el tratamiento de los datos es ilícita, o sea ilegal, y ha de poder demostrar dicho responsable, que las actividades de tratamiento son conformes con el Reglamento General, con la LOPDGDD, y en su caso con el Convenio Colectivo, y que además las medidas adoptadas son eficaces.

B) Finalidad a la hora de recabar los datos:

Los datos de carácter personal no se piden, ni se recaban, ni se tratan, sin una finalidad y un motivo o causa, sobre todo porque lo que está en juego son derechos fundamentales que hay que proteger.

Desde el punto de vista del derecho de protección de datos, este es un derecho fundamental, como ya sabemos, y dicho derecho hay que protegerlo, por eso:

1. ni deben recabarse datos excesivos,
2. ni deben recabarse fuera de determinado ámbito,
3. ni vale el consentimiento sino ha existido información previa, ni fines adecuados, o una norma que permita pedirlos, recabarlos y tratarlos.

Y cumpliendo lo anterior además hay que establecer medidas adecuada para proteger dichos datos. Dichas medidas deben tener en cuenta:

- la naturaleza,
- el ámbito,
- el contexto y
- los fines del tratamiento,
- así como los riesgos para los derechos y libertades de los trabajadores y trabajadoras.

Porque pueden existir otros derechos fundamentales que pueden verse afectados a la hora de recabar datos de carácter personal como el derecho a la imagen, a la libertad de tránsito, a la libertad de expresión, a la libertad sindical, al derecho de huelga, incluidas las actuaciones de los piquetes de huelga que forman parte del contenido esencial del derecho de huelga.

C) Principios:

No se pueden recoger datos de los trabajadores sin causa y base legal. Y no se pueden recoger y tratar los datos de los trabajadores sin información previa, porque aunque se pida el consentimiento este no es válido si antes no ha existido información previa y la aplicación de los principios del Reglamento.

El deber de información forma parte del contenido esencial del derecho a la protección de datos. **Este deber de información existe tanto para recoger datos de los trabajadores y trabajadoras para un tratamiento que no requiera consentimiento, como en el supuesto de que sí lo requiera**. A este respecto, en el caso de existir contradicción en determinados postulados, entre el Reglamento y la LOPPGDD, prima el Reglamento, y la regulación en contra del mismo es inaplicable, debiendo el juez nacional inaplicar cualquier norma interna que incurra en contradicción.[19]

Los empresarios con carácter general, deben tener siempre presente los principios fundamentales de protección de datos, independientemente de la tecnología utilizada; de tal manera que[20]:

- **es muy poco probable que el consentimiento constituya una base jurídica para el tratamiento de datos en el trabajo**, a no ser que los trabajadores puedan negarse sin consecuencias adversas,

- **la dependencia que resulta de la relación empresario/trabajador, impide rara vez que el trabajador o trabajadora esté en condiciones de dar, denegar o revocar el consentimiento libremente**. Salvo en situaciones excepcionales, los empresarios tendrán que basarse en otro fundamento jurídico distinto del consentimiento, como la necesidad de tratar los datos para su interés legítimo,

  pero **un interés legítimo en sí mismo tampoco es suficiente** para primar sobre los derechos y libertades de los trabajadores,

- **en ocasiones, el empresario puede invocar la ejecución del contrato de trabajo y los intereses legítimos, pero siempre que el tratamiento sea estrictamente necesario para dicho fin legítimo y respete los principios de proporcionalidad y subsidiariedad,**[21]

- **independientemente de la base jurídica de dicho tratamiento, antes de su inicio, se debe realizar una prueba de proporcionalidad** con el fin de determinar si el tratamiento es necesario para lograr un fin legítimo, así como las medidas que deben adoptarse para garantizar que las violaciones

de los derechos a la vida privada y al secreto de las comunicaciones no se produzcan. (Se limiten al mínimo),

- el contenido de las **comunicaciones electrónicas** realizadas desde establecimientos empresariales goza de la **misma protección** de los derechos fundamentales que las comunicaciones **analógicas**,[22]

- en relación con interferir en los dispositivos que se entregan a los trabajadores, el grupo de trabajo del art. 29 pidió que en el Reglamento se estableciera una excepción adecuada para no interferir en las comunicaciones de los trabajadores. **El consentimiento** de los trabajadores en este aspecto, es de **dudosa validez,**[23]

- **los trabajadores deben recibir información efectiva** sobre el **control** que se lleva a cabo,

- cualquier **transferencia internacional** de datos de los trabajadores únicamente debe efectuarse cuando esté garantizado un **nivel adecuado de protección**,

- se requiere una nueva evaluación del equilibrio entre el interés legítimo del empresario de proteger su empresa y la expectativa razonable de privacidad de los interesados: los trabajadores. (***La llamada ponderación***). Garantizar que los datos se tratan con **fines específicos y legítimos y que sean proporcionados y necesarios**,

- hay que tener en cuenta el principio de limitación de la finalidad y al mismo tiempo asegurarse de que los datos sean **adecuados, pertinentes y no excesivos** para la finalidad legítima,

- aplicar los principios de **proporcionalidad y subsidiariedad**, independientemente del fundamento jurídico aplicable,

- ser transparentes con los trabajadores sobre el **uso y la finalidad de las tecnologías de control**,

- permitir **el ejercicio de los derechos del interesado**, incluidos el derecho de acceso y, en su caso, la rectificación, supresión o bloqueo de datos personales, y revocar el consentimiento,

- mantener la exactitud de los datos y no conservarlos más tiempo del necesario, y

- **adoptar todas las medidas** necesarias para proteger los datos contra el acceso no autorizado (derechos SOPLAR, ya no ARCO),

- así como garantizar que el personal conozca suficientemente las obligaciones en materia de protección de datos.

EN RESUMEN, los empresarios deben, por tanto, tener en cuenta lo siguiente en relación con los datos de los trabajadores y trabajadoras:

- para la mayoría de los datos que se recaban por las empresas en el trabajo, la base jurídica no puede y no debe ser el consentimiento de los trabajadores y trabajadoras debido a la especial naturaleza de la relación entre empresario y trabajador,

- el tratamiento de los datos personales, puede ser necesario para la ejecución del contrato de trabajo, y con respecto al cumplimiento de las obligaciones legales relativas a la ejecución de dicho contrato,

- aunque, es bastante común que el Derecho laboral pueda imponer obligaciones jurídicas (o convencionales) que requieran el tratamiento de datos personales; en tales casos, el trabajador debe estar clara y plenamente informado de dicho tratamiento (a menos que sea de aplicación una excepción),

- en caso de que un empresario pretenda invocar un interés legítimo para recabar datos del trabajador y su consentimiento inclusive, la finalidad del tratamiento debe ser:
  - legítima,
  - el método elegido o la tecnología específica deben ser necesarios, proporcionados,
  - y aplicados de la manera menos intrusiva posible,
  - y el empresario deberá poder demostrar que se han adoptado las medidas adecuadas para garantizar un equilibrio (adecuado) con los derechos y libertades fundamentales de los trabajadores (ponderación);

- las operaciones de tratamiento deben cumplir también los requisitos de:
  - transparencia,
  - y los trabajadores deben estar clara y plenamente informados del tratamiento de sus datos personales, incluida la existencia de cualquier pretendido control de su actividad laboral, [24]
  - debiendo adoptarse medidas técnicas y de organización adecuadas con el fin de garantizar la seguridad del tratamiento.

Como debe ser la declaración de consentimiento, cuando es necesario

Con carácter general, el consentimiento que determina como válido el RGPD es el consentimiento que debe darse mediante un acto:

- afirmativo
- claro
- que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado,

de aceptar el tratamiento de datos de carácter personal que le conciernen, debiendo poder ser acreditada por lo que debe constar:

1. como una declaración por escrito,
2. inclusive por medios electrónicos,
3. una declaración verbal[25],
4. para que el consentimiento sea válido, también debe ser revocable.[26]

No vale como consentimiento

No decir nada, o no hacer nada y, por lo tanto, el silencio, o pretender que el consentimiento sea tácito, eso no es una declaración de consentimiento.

Incluso desde el 25 de mayo de 2018, se deber recabar un nuevo consentimiento del afectado, a menos que pueda considerarse el tratamiento amparado en la regla de ponderación establecida en el artículo 6.1 f) del RGPD.

Cuando un empresario tiene que tratar datos personales de sus trabajadores, es engañoso partir del supuesto de que el tratamiento puede legitimarse a través del consentimiento de estos.

En los casos en que un empresario dice que se requiere el consentimiento y existe un perjuicio real o potencial relevante derivado del hecho de que el trabajador no consienta (lo cual puede ser muy probable en el contexto laboral, especialmente cuando el empresario hace un seguimiento del comportamiento del trabajador a lo largo del tiempo), entonces el consentimiento no es válido, ya que no es y no puede ser dado libremente.

Por tanto, insistimos que, en la mayoría de los casos de tratamiento de datos de los trabajadores, la base jurídica de dicho tratamiento no puede y no debe ser el consentimiento de los trabajadores, por lo que se requiere una base diferente.

Incluso en los casos en que el consentimiento pueda considerarse una base jurídica válida de dicho tratamiento (es decir, si se puede concluir sin ninguna duda de que el consentimiento se ha dado libremente), éste debe ser una manifestación específica e informada de la voluntad del trabajador.

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

El interés legítimo del empresario

Una segunda posibilidad del tratamiento de datos, la constituye la existencia de un interés legítimo. La nueva norma europea, el RGPD, contempla como causa legitimadora para el tratamiento de datos: el interés legítimo, según su artículo 6.1.f).

Para determinar si procedería la aplicación del citado precepto habrá de aplicarse la regla de ponderación prevista en el mismo; es decir, será necesario valorar si en el supuesto concreto objeto de análisis, existiría un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, valorando si debe prevalecer el interés legítimo o los derechos y libertades fundamentales del trabajador o trabajadora, que requieran protección conforme a lo dispuesto en el artículo 1 del RGPD, o si, por el contrario, los derechos fundamentales o intereses de los trabajadores o trabajadoras, a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo en que el responsable o el tercero pretende fundamentar el tratamiento o la cesión de los datos de carácter personal.

El RGPD, enumera algunos supuestos que pueden ser tomados en consideración para determinar la aplicabilidad de dicha regla:

Así, en primer lugar, se señala que el interés legítimo “podría darse”, por ejemplo:

- cuando existe una relación pertinente y apropiada entre el trabajador y trabajadora y el responsable, y con una finalidad definida,

- o, el tratamiento de datos de carácter personal es estrictamente[27] necesario para la prevención del fraude.

Por otra parte, el considerando 48 añade que "los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados".

Finalmente, el considerando 49 añade un ejemplo más, al señalar que "constituye un interés legítimo del responsable del tratamiento, el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema de información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad".

En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de "denegación de servicios" y daños a los sistemas informáticos y de comunicaciones electrónicas".

Como puede comprobarse, el propio Reglamento establece los criterios básicos a tomar en consideración para poder detectar intereses legítimos que permitan valorar la aplicación de la regla de equilibrio establecida en el artículo 6.1 c).

Sin embargo, "conviene no confundir la legitimidad del fin con la constitucionalidad del medio para su consecución", ya que "esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, y (…) se confundiría la legitimidad del fin (…)por lo que son necesarios los principios de proporcionalidad, idoneidad e intervención mínima,[28] en lo que respecta a pretender utilizar un interés legítimo en relación con los trabajadores y trabajadoras.

Es decir, por mucho que exista un pretendido interés legítimo por parte del empresario, también tiene que ser legítimo y constitucional la forma de

protegerlo, ya que cualquier conveniencia empresarial no es un interés legítimo, además de que, para poder proteger dicho interés puede haber un sinfín de formas y medidas, pero solo valen si se van a utilizar aquellas medidas que utilizando datos de carácter personal, sean proporcionales, idóneas, se haya probado la regla de ponderación entre los derechos en conflicto, y se hayan establecido teniendo en cuenta el principio de intervención mínima.

Los trabajadores pueden negarse a otorgar su consentimiento, y pueden revocarlo[29]

¿Qué pasa si un grupo de trabajadores no consienten o revocan el consentimiento sobre que ya no se les monitorice por ejemplo, el uso de su ordenador en las redes sociales, habiendo existido un acuerdo con la representación de los trabajadores en sentido positivo, o habiendo dado su consentimiento individualmente? O ¿en el móvil o la Tablet? ¿O la huella dactilar, convertida en digital por un programa especial para fichar? ¿Qué pasa si deciden de pronto negarse a que sus datos personales sean transferidos internacionalmente a un país sin las debidas garantías en la materia? En ese caso, el interés legítimo del empresario sería alegado de forma inmediata y en este caso el convenio colectivo puede ser una norma adecuada y de carácter previo para regular los derechos en conflicto.

Porque no estaría claro, si no hay una norma jurídica y si no hay un interés legítimo que fuera válido el comportamiento empresarial, y sobre todo si, aunque se alegue dicho interés legítimo y se pretenda recabar el consentimiento del trabajador, no se cumplen los principios que se han alegado en este trabajo como fundamentales según la norma europea, porque son muchos los derechos fundamentales en conflicto, sobre todo los de los trabajadores, y por qué inclusive la información previa tampoco avalaría el comportamiento del empresario.

El grado de cumplimiento normativo

En todo caso, es necesario que el responsable del tratamiento a la hora de realizar el análisis previo y los posibles riesgos y afectación de los derechos en conflicto, cumpla con la normativa europea y nacional.

En la “lista de verificación” del grado de cumplimiento normativo realizado por la AEPD, incluido en el documento denominado: “Guía listado de cumplimiento de la AEPD”, se incluye un catálogo para comprobar, si el tratamiento de que se trate, cumple con la licitud o no correspondiente, o si se han cumplido las condiciones para obtener el consentimiento, así como el tratamiento de las

categorías especiales de datos, incluso si es necesario para el cumplimiento de las obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la Seguridad Social, incluida la protección añadida, en la medida que exista un convenio colectivo con arreglo a derecho, entre otras cuestiones.[30] Listado que puede ser muy útil para los representantes de los trabajadores en la protección del derecho.

Con carácter previo es necesario señalar que, el legislador ha sido poco receptivo a las demandas de las organizaciones sindicales a este respecto. No ha existido ningún contacto previo, ni reuniones al respecto con los interlocutores sociales sobre cómo podría implementarse la norma.

Desde luego para UGT se ha perdido una importante oportunidad para regular el concepto de derechos digitales, y un contenido más adecuado a la realidad existente sobre todo en el ámbito de las relaciones laborales.

De ahí que consideremos necesario que los convenios colectivos ejerzan el papel que les ha encomendado el legislador comunitario, para evitar que la parquedad de las normas en este sentido y su posible contradicción inclusive con el RGPD, determinen que aumente la conflictividad en esta materia, o se vulneren gravemente los derechos de los trabajadores.

Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral

De carácter general

El art. 87 de la nueva LOPDGDD, viene a establecer con carácter general, la protección del derecho a la intimidad en el uso de los dispositivos digitales puestos a disposición por un empleador.

Sobre dicha protección es necesario traer a colación el Convenio europeo de derechos humanos y determinadas sentencias dictadas por el TEDH.

- El art. 8 del Convenio europeo de derechos humanos (CEDH), protege el respeto a la vida privada y a la correspondencia.

- La sentencia Barbulescu II dictada por parte de la Gran Sala del TEDH rectificó la doctrina de la sentencia anterior Barbulescu I (dictada por la Sección Cuarta de dicho tribunal) estableciendo la vulneración del derecho a la intimidad del trabajador, si se accedía a la cuenta de mensajería instantánea de un trabajador en la que existían mensajes de contenido privado, pese a ser propiedad de la empresa.

Con esta sentencia parece claro que el TEDH mantiene un concepto amplio de vida privada, que también se proyecta en las relaciones sociales dentro de la relación laboral. La propia sentencia habla de “private social life”.

Consideró además que la normativa interna de la empresa no podía reducir la vida privada social dentro del puesto de trabajo "a cero", por lo que subsiste una expectativa razonable de privacidad a pesar de la existencia de una prohibición expresa y reiterada de uso de los medios informáticos de la empresa con fines personales. "La mensajería electrónica enviada desde una cuenta profesional debe considerarse correspondencia".

La sentencia Barbulescu II determinó que las garantías no solo deben existir en la legislación laboral sino también en la penal o civil, por lo que pueden determinarse en los convenios colectivos y "deben ser y tener un componente de garantía de dicho derecho".

Además, especialmente señaló que "los jueces nacionales deben examinar si el trabajador ha sido informado previamente de la posibilidad de que el empresario aplique medidas de control de las comunicaciones y además la notificación debe ser clara sobre la naturaleza de las medidas de control", lo que se desarrolla en el RGPD mediante el principio de transparencia.

La Gran Sala especificó que " los controles que supongan un acceso por parte del empresario al contenido de las comunicaciones deben someterse a un control de proporcionalidad más intenso", de tal manera que se debe hacer un examen más estricto de dicha proporcionalidad, del control empresarial y de los fines que justificarían el acceso al contenido de los mensajes ***de un trabajador o trabajadora*** y sobre la existencia de "medios alternativos de control menos restrictivos de la privacidad del trabajador".

- También es importante tener en cuenta las instrucciones de la AEPD, tal y como hace la sentencia López Ribalda, que tiene en cuenta la Instrucción 1/2006, de 8 de noviembre, de tal manera que la existencia de "cámaras ocultas" o no ser informado aunque sea de una manera genérica, "debiendo tener un objetivo específico y no prolongarse en el tiempo", no permite el control por parte del empresario de los trabajadores con nuevas tecnologías, sobre todo con el uso de datos biométricos, sino que estos deben ser el último recurso.
- La relación de la sentencia anterior con la dictada por el Tribunal Constitucional en el caso Berska STC 39/2016, de 3 de marzo, se centra en el análisis del deber de información, cuando es mínimo, adecuado o suficiente.
- En el Caso Libert contra Francia (STEDH de 22 febrero 2018), en cambio, no existe violación del art. 8 del CEDH, por acceder la empresa pública SNCF, a los archivos del ordenador del trabajador, sin que se plantee el tema del derecho a la información previa, sino solo si existían garantías internas para no poder abrir los correos electrónicos personales del trabajador.

Desde luego el derecho a la intimidad es un derecho fundamental y un derecho humano. La revolución 4.0, en este aspecto, va a ser una de las cuestiones más preocupantes con respecto al individuo, sobre todo la intromisión en su derecho a la intimidad. Garantizar el equilibrio entre derechos fundamentales, la autodeterminación informativa y la privacidad y la libertad de empresa, de expresión etc. va a ser una constante en las relaciones de trabajo, y sobre esto el papel del convenio colectivo es fundamental.

De carácter específico

Pero también establece el artículo inicial de este apartado que: "los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado".

Sin duda, este precepto parece entrar en contradicción con la redacción del RGPD, que determina que será **la legislación nacional o los convenios colectivos** los que deben proceder a realizar tal regulación, por dos razones:

- porque lo regulado en el mismo se refiere de forma muy genérica e inconcreta a cuestiones resueltas por nuestra jurisprudencia constitucional que hasta el momento es anterior al RGPD,
- porque señala que los empresarios "deberán regular", pero no tiene en cuenta que la ley o los convenios, según el RGPD son los habilitados para establecer dicha regulación,
- y porque habla de que, en su elaboración, deberán participar los representantes de los trabajadores, lo que parece legitimar la entrada a nivel de empresa solamente de la participación de los representantes. Pero el mayor nivel de participación de los mismos es el convenio colectivo, y si la participación es tal y no es información y consulta de los representantes, la entrada debe ser del convenio colectivo, convenio colectivo cuyo ámbito de actuación no se limita en el RGPD, que señala "convenios colectivos

incluidos los convenios de empresa", y es a todos los niveles, desde el convenio colectivo sectorial estatal desde el que debe darse la participación de todos los representantes de los trabajadores incluidos los sindicatos.

De ahí que UGT considera necesario establecer en la negociación de los mismos lo siguiente:

- Se regulará por convenio colectivo cualquier determinación relativa a los dispositivos digitales puestos a disposición de los trabajadores, evitando la limitación para uso particular de los mismos, dada la necesidad de "vida social laboral", que también se desarrolla dentro del ámbito de las nuevas tecnologías y con el uso de cualesquiera dispositivos digitales, en las relaciones de trabajo.

- En el caso de que se establezca una limitación temporal en dicho uso y para fines privados se determinará expresamente que la misma se refiere a circunstancias relativas a la posibilidad de competencia desleal a la empresa o al ejercicio de funciones relativas a otros trabajos que pudieran ser objeto de pluriempleo por parte del trabajador, por ejemplo.

- En todas las regulaciones que se determinen en los convenios colectivos se tendrán en cuenta los principios del RGPD, así como la proporcionalidad, y ponderación de las cuestiones sometidas a regulación.

- No se podrá acceder al contenido de los dispositivos digitales ni monitorizar los mismos con carácter general, salvo que existan sospechas fundadas de cometerse un ilícito penal o laboral y previa su tipificación en el convenio colectivo dentro del sistema de faltas y sanciones. En ese caso y antes de realizarse dicha monitorización se comunicará a los representantes de los trabajadores, así como con carácter previo al trabajador, sobre el que se tienen fundadas sospechas, debiendo existir siempre, por lo tanto, información previa.

- No serán válidas las determinaciones genéricas convencionales del posible control o monitorización de los dispositivos digitales.

- Hasta tanto exista una jurisprudencia consolidada, se acudirá a la jurisprudencia anterior al RGPD, que en parte ha recogido en el apartado tercero del art. 87 del mismo, la necesidad de su elaboración con los representantes de los trabajadores, aunque teniendo en cuenta la dicción del RGPD, la UGT, considera necesario establecer la regulación principal en el convenio colectivo correspondiente, primándose el convenio colectivo

sectorial estatal en las cuestiones generales garantes de los derechos fundamentales.

El por qué los convenios colectivos deben regularlo es por las siguientes razones:

1. Porque el mayor instrumento de participación de los representantes de los trabajadores y de los sindicatos y las organizaciones empresariales y las empresas, es el convenio colectivo.

2. Porque el propio considerando 155 del RGPD, norma de aplicación directa, prima por encima de la LOPDGDD, señalando que : (155) "El Derecho de los Estados miembros o los convenios colectivos, incluidos los convenios de empresa", pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.

3. Porque la dicción del art. 88 del RGPD es clara, y por lo tanto, el convenio colectivo tiene un papel fundamental allí donde la ley no ha realizado una regulación específica.

   En este caso, el convenio colectivo deberá regularlo siembre sobre la finalidad de protección del derecho de protección de datos de los trabajadores y trabajadoras, así como la protección de su intimidad y privacidad también teniendo en cuenta lo siguiente:

   a) En el caso de que se ponga a disposición de los trabajadores dispositivos digitales tales como ordenadores, PC, portátiles, Smartphones, tablets, MP3, dispositivos con disco duro, video portátil, consolas, PDA, Mcbook, etc., no se podrá acceder a los contenidos de tales dispositivos digitales con carácter general ni de forma directa, ni de forma indirecta mediante el uso de cualquier tipo de software que pretenda el seguimiento del tiempo de trabajo de los empleados, que tipo de aplicaciones están utilizando, ni controlar

de manera individual ni simultánea un número limitado o ilimitado de ordenadores, dispositivos, ni realizar análisis de rendimiento, ni informe de productividad etc.

b) Se pueden establecer sistemas de no acceso (capado) a determinadas págs. web previa información contenida en el convenio colectivo.

c) En el caso de que un trabajador sea sancionado como consecuencia de una conducta inadecuada o ilícita dentro del ámbito laboral, se deberá contemplar en el sistema de faltas y sanciones el derecho a eliminar de su expediente sancionador dichos datos de carácter personal, por lo que la sanción no deberá servir, para la determinación de otra sanción posterior.

Derecho a la desconexión digital en el ámbito laboral

El art. 88 del RGPD, viene a regular el derecho a la desconexión digital en el ámbito laboral:

"1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de 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. 2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores. 3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas".

La redacción inicial de este artículo, no deja de ser un tanto confusa. Que los trabajadores y trabajadoras, tienen derecho a desconectar, de la manera que sea, o a que su jornada de trabajo se dé por terminada es una obviedad. Y no se define que se entiende por desconexión digital, o se conceptúa en que consiste dicho derecho.

No parece, por tanto, que, pese a la dicción de la norma y el reconocimiento formal del derecho a la desconexión, se establezca un concepto jurídico del mismo.

La jornada de trabajo se regula tanto en el ET, como en los convenios colectivos y la regulación jurídica de carácter especial sectorial correspondiente, regulación y determinación de la jornada que se concreta en el calendario laboral, que hace conocer exactamente cuál es la jornada de los trabajadores, incluida la distribución y el horario de trabajo, independientemente de la realización o no de horas extraordinarias del tipo que sean, o de horas complementarias en el correspondiente contrato a tiempo parcial, o de los tiempos de presencia, tiempos a disposición del empresario, etc., hace conocer a empresario y trabajador, cual es la jornada de trabajo.

Si la jornada se incumple por parte del empresario, ya existen mecanismos más que suficiente en la legislación laboral, para denunciar al empresario o realizar la reclamación judicial de los derechos.

La LOPDGDD, no define lo que es conexión ni desconexión digital. Lo único que se señala es que "las modalidades del ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral". Pero el derecho a conocer el inicio y el fin de la jornada laboral ya existía, ¿qué derecho es éste?

En algunos convenios colectivos conscientes del problema del exceso y uso y abuso de las nuevas tecnologías, sobre todo por la facilidad en el tiempo y en el espacio del uso de las mismas, se ha procedido a regular de una manera muy inadecuada.

Por ejemplo, en el convenio colectivo de AXA SEGUROS para los años 2017 a 2020 se ha establecido, (…) un cierto derecho a la desconexión digital de la siguiente manera: "las partes firmantes de este convenio coinciden en la necesidad de impulsar el derecho a la desconexión digital una vez finalizada la jornada laboral. Consecuentemente, salvo causa de fuerza mayor o circunstancias excepcionales, AXA reconoce el derecho de los trabajadores a no responder a los mails o mensajes profesionales fuera de su horario de trabajo".

¿Por qué es inadecuada esta forma de regularlo? Porque las "normas sociales de la UE, y su jurisprudencia entre ellas STJUE de 10 de septiembre de 2015, C-266/14) y nuestra Constitución Española, en los arts. 18.4, 10, 15 y 40, para la protección eficaz de la salud psicosocial de los trabajadores, y conforme a la doctrina constitucional, por ejemplo, STC 62/2007, de 27 de marzo, ya

habilitaban a todo trabajador que no quiera responder fuera de su horario de trabajo, a no hacerlo.

Además "es doctrina constitucional española que, toda concepción, empresarial y social que considere el tiempo libre del trabajador como tiempo vinculado al interés productivo del empleador, es inconstitucional, porque reduce a simple factor de producción a la persona del trabajador".

Aunque, esta doctrina constitucional se fijó en relación al periodo de vacaciones (STCo 193/2003, 27 de octubre), realmente tiene una dimensión general y ha de servir para toda comprensión de los periodos de descanso.

En todos ellos con una mayor o menor intensidad, se considera un mismo fin: "el tiempo de descanso es un tiempo de reposición de energías y de esparcimiento propio, por lo tanto, exige, por sí mismo, la garantía de una libertad de desconexión respecto del tiempo productivo".

En la STSJ de Cataluña 3613/2013 de 23 de mayo, en el supuesto de hecho que se resuelve en la misma, se había instalado un acelerómetro en los móviles de los trabajadores, además de un GPS, para el control de su actividad laboral. La empresa pretendía justificarlo para tener conocimiento en el caso de un eventual accidente, debiendo cargarse dicho dispositivo, en casa. La sentencia señala que se vulneran los derechos relativos a la esfera personal y privada del trabajador, que debe continuar en una situación "in vigilando del dispositivo para que esté en condiciones óptimas", ***de funcionamiento***.

"Fuera de la jornada laboral (...) lleva consigo un perjuicio en su salud por (...) estar pendiente del citado dispositivo, y la incidencia que ello tiene no solo para él sino también en lo que es esa esfera privada personal familiar en la que la empresa demandada, no puede tener interferencia alguna, ni siquiera por motivos tecnológicos, (…), pues está fuera de la jornada laboral".

Esto ya pone en evidencia, que lo que no debe hacer el empresario es precisamente, o bien directamente o bien a través de sus Directivos, romper el descanso del trabajador.

Lo que se debe evitar y prohibir es el envío por parte de las empresas y fuera de los tiempos de trabajo, de mensajes de mensajería instantánea, correos electrónicos, chats en el Messenger o a través de cualesquiera aplicaciones incluido el WhatsApp, tan de moda en los últimos tiempos de mensajes con órdenes de trabajo, por el estrés que se infringe a los trabajadores, porque la resultante no solo es la enfermedad psicosocial de las personas trabajadores

sino la intromisión constante y permanente en su vida personal y su tiempo libre, aunque dichas ordenes por supuesto, no tenga que ser ejecutadas fuera de la jornada de trabajo, pero solo el stress y la atención necesaria que se presta a la hora de recibirlos, ya perturba el descanso y por lo tanto, el tiempo libre de los trabajadores.

Ya hay numerosas empresas que reconocen el sistema "Mail onholiday", para que los correos enviados a trabajadores de vacaciones sean automáticamente redirigidos a otros disponible de la empresa. De este modo se producen dos efectos: se evita que lleguen a sus destinatarios en vacaciones -desconexión propiamente-, y también se evita la sobrecarga de mensajes propia de la acumulación en el período de vacaciones, efecto preventivo del estrés postvacacional.

Para conseguir un buen uso de los dispositivos digitales, algunas empresas, como ya sucede con la iniciativa legislativa francesa sobre desconexión digital, prohíben enviar mensajes a los empleados bajo el riesgo de sanciones disciplinarias, desde leves hasta el despido.

Si la jornada de trabajo y los tiempos de trabajo efectivo incluidos los descansos y vacaciones se regulan en el convenio colectivo de que se trate, de la misma manera debe establecerse el derecho de desconexión, por las implicaciones que tiene sobre la vida privada y sobre todo, sobre la conciliación de la vida personal y familiar, independientemente de que la norma diga: mediante la negociación colectiva o en defecto por acuerdo entre los representantes de los trabajadores y la empresa.

También es sorprendente que sea previa audiencia de los representantes de los trabajadores la pretensión en la LOPDGDD que se articule este derecho, cuando el RGPD se refiere a los convenios colectivos.

En este sentido la aplicabilidad directa del Reglamento está por encima, en consecuencia, debe ser los convenios donde se produzca la regulación, sobre todo porque la "audiencia" es rebajar el contenido del derecho de participación de los representantes de los trabajadores.

Y además afecta a otros derechos, muy importantes, por ejemplo, a la conciliación de los derechos laborales y personales, sobre todo en relación con el interés del menor, cuando de reducciones de jornada se trata, porque las familias, los hijos y por lo tanto, la conciliación, no debe verse afectada por un ***supuesto mensaje de whassap*** con órdenes empresariales.

Por otra parte, en el caso del derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, o del teletrabajo y deben observarse las consideraciones de los documentos realizados por UGT para el teletrabajo y tener en cuenta el contenido del Acuerdo Marco europeo sobre teletrabajo.

De ahí que se podría determinar en los convenios colectivos que por ejemplo, una vez terminada la jornada laboral, los representantes del empresario están obligados a respetar los tiempos de descanso (incluso dentro), fuera de la jornada laboral, y tanto tiempos de descanso de carácter diario, semanal, o mensual, como el descanso por vacaciones o durante los tiempos de suspensión de la relación laboral, como los periodos de incapacidad temporal, sin que quepan tareas, ni labores de mantenimiento de los dispositivos digitales, tecnológicos o cualesquiera otros fuera de la jornada de trabajo.

Para evitar la vulneración del derecho de descanso se prohíbe la realización de llamadas telefónicas, el envío de mensajes de mensajería instantánea o mediante el correo electrónico o cualesquiera otros que impidan el ejercicio de dicho descanso.

Dentro del sistema de faltas y sanciones se tipificará como tal el incumplimiento de las anteriores determinaciones.

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

Los empleadores podrán tratar las imágenes de los trabajadores y trabajadoras para ejercer funciones de control, según el art. 89 de la LOPDGDD, siempre y cuando dichas funciones de tratamiento y de control, se ejerzan dentro de la normativa y con los límites inherentes al mismo.

La videovigilancia sigue presentando los mismos problemas para la privacidad de los trabajadores que antes: la capacidad de grabar de forma continuada el comportamiento del trabajador.

Los cambios más relevantes relacionados con la aplicación de esta tecnología en el contexto del empleo son la capacidad de acceder fácilmente a los datos recogidos a distancia (por ejemplo, a través de un teléfono inteligente), la reducción de los tamaños de las cámaras (junto con un aumento de sus capacidades, por ejemplo, de alta definición) y el tratamiento que pueden realizar los nuevos análisis de vídeo.

Con las capacidades que ofrecen los análisis de vídeo, por ejemplo, es posible que un empresario observe las expresiones faciales del trabajador por

medios automatizados, identifique desviaciones con respecto a los patrones de movimiento predefinidos (por ejemplo, una fábrica), etc. Esto sería desproporcionado a efectos de los derechos y libertades de los trabajadores y, por tanto, ilegal en general.

El tratamiento también puede implicar la elaboración de perfiles y, posiblemente, la toma de decisiones interesadas. Por tanto, los empresarios deben abstenerse de utilizar tecnologías de reconocimiento facial con carácter general. Puede haber algunas excepciones a esta regla, pero tales escenarios no pueden utilizarse para invocar una legitimación general del uso de estas tecnologías.

Una imagen es un dato biométrico, como lo es la firma manuscrita y la huella dactilar, y en virtud del art. 9 del RGPD, queda prohibido el tratamiento de los datos biométricos que estén dirigidos a identificar de manera inequívoca a una persona física, salvo en determinadas circunstancias.

El artículo 89 de la LOPGDD ha venido a establecer que: "1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica. 2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos. 3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley".

El artículo 22 en su apartado final remite al art. 89 para regular la videovigilancia en el lugar de trabajo, estableciendo que en el caso de la conservación de las imágenes, si se tendrá en cuenta el apartado 3 de dicho artículo 22[31]

Además, se reforma el art. 20. bis del ET en los siguientes términos: "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", y se añade una nueva letra j bis) en el artículo 14 del Texto Refundido de la Ley del Estatuto Básico del Empleado Público, señalando el derecho a: "la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".[32]

La videovigilancia ya ha sido objeto de la primera sentencia en los Juzgados de lo Social de Pamplona, determinando que en el RGPD no se establece ninguna excepción relativa al deber de transparencia y de información previa, en materia de protección de datos en las relaciones laborales, por lo que determinadas excepciones que parece realizar la LOPDGDD, serían inaplicables por la aplicabilidad directa del Reglamento.

Si analizamos el art. 89 LOPGDD, más detenidamente, podemos visualizar algunas cuestiones importantes, dejando al margen algunas otras cuya determinación ya es conocida, ya sea por las normas anteriores, ya sea por la jurisprudencia constitucional, pero las relatadas a continuación merecen un comentario:

1. los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control,
2. siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo,
3. los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, (a los trabajadores y empleados públicos y a los representantes),
4. en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo, *(de información de captación de imágenes)*,
5. la grabación de sonidos en el lugar de trabajo, se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones,

bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores.

En relación con el primer y el segundo apartado anterior, el considerando 26 del RGPD señala que los principios de protección de datos deben aplicarse a "toda información", determinando en el art.4 apartado 1, que son datos de carácter personal con gran amplitud y por lo tanto, la imagen y la voz de una persona lo son.

Si los principios del RGPD, y de la LOPDGDD, deben aplicarse a todos los datos de carácter personal, la resultante es que **en principio debe respetarse el principio de "proporcionalidad" con carácter prioritario como con cualquier otro dato**.

Esto significa que **hay que valorar** a la hora de controlar la actividad de los trabajadores, **otros medios menos intrusivos en su intimidad y en otros derechos y libertades, como en este caso puede ser el derecho a la imagen, y a la libertad de tránsito, expresión etc., y de actividad social inclusive en el entorno de trabajo**.

De la misma manera se debe aplicar **el principio de minimización de datos** recogido en el art. 5 del RGPD, de manera que sean: **pertinentes, adecuados y limitados** en relación con los fines para los que son tratados.

De ahí, **que solamente la videovigilancia sería una medida proporcional y justificada si se cumplen los siguientes requisitos**:

1. Que se trate de una medida susceptible de conseguir el objetivo propuesto.
2. Que no exista otra medida **más moderada** para la consecución de tal propósito con igual eficacia.
3. Que la misma **sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general**.

La propia AEPD, ha señalado a este respecto que el hecho de que por ejemplo, se legitime la videovigilancia por razones de seguridad, no implica necesariamente que se legitime la grabación de la voz, tratamiento que tendría que tener justificación propia, y en todo caso en la concreción del principio de proporcionalidad se encontrará el derecho a la intimidad, honor y propia imagen de las personas, de forma **que resultará desproporcionada la captación de imágenes que puedan afectar a dichos derechos o la escucha o grabación de conversaciones**.[33]

Además, utilizando **la regla de ponderación** será necesario valorar **si** en el supuesto concreto al que se refiera la instalación de un sistema de videovigilancia **existe un interés legítimo** perseguido por el responsable del tratamiento **que prevalezca** sobre el interés o los derechos y libertades fundamentales de los trabajadores y trabajadoras, **o no**.

Por lo tanto, es necesario tener en cuenta que varios principios pueden ser vulnerados a la hora de establecer sistemas de videovigilancia de los trabajadores y la posible vulneración del principio de proporcionalidad en la videovigilancia y captación de la imagen y voz de empleados (y personas que acceden a edificios), lo que puede hacer que esos sistemas no sean válidos.[34]

En relación con el apartado tercero arriba numerado, es necesario señalar lo siguiente, sí los sistemas de videovigilancia para el control empresarial solo se adoptarán cuando existe una relación de proporcionalidad entre la finalidad perseguida y el modo en que se traten las imágenes, y no haya otra medida más idónea, **el derecho de información a la representación de los trabajadores y a los trabajadores no puede ser residual, ni un extracto o comunicación de la necesidad de control, ni un somero cartel en el que se alerte de que determinada zona está siendo sometida a videovigilancia**.

Ello es así, porque la propia AEPD determina que la información debe ser de carácter personal y que se garantice la recepción de la misma y no podrá efectuarse a direcciones particulares ni a móviles privados por ejemplo, y por supuesto, se debe poner a disposición de los afectados la información del art. 13 del RGPD.[35][36]

Por otra parte, pese a que se habla del derecho de información previa y audiencia previa de los representantes de los trabajadores en la LOPGDD, en el RGPD, se habla de "convenios colectivos", convenio colectivo que es el instrumento normativo y participativo más importante de la acción sindical y una de las facultades que forman parte del contenido esencial del derecho de libertad sindical, y por lo tanto, debe primar la regulación que este establezca y la prevalencia de promover en los mismos la defensa de los derechos de protección de datos de los trabajadores, junto con otros derechos fundamentales como la imagen, insistimos.

Por ello, con carácter general, la UGT **considera que este método de control de las relaciones de trabajo, deber regularse en los convenios colectivos, debe utilizarse de forma residual y atendiendo a los principios y finalidades que se establecen en el RGPD**, no pudiendo utilizarse con carácter general para funciones de control de los trabajadores y empleados públicos, y no admitiéndose sistemas de grabación de sonidos.

De la misma manera no se podrá utilizar ningún sistema de grabación de imágenes de los trabajadores para usos de la empresa ya sean publicitarios o de marketing, ni de forma directa ni indirecta con su exhibición en redes sociales, salvo que por convenio colectivo o acuerdo individual de trabajo se retribuya el derecho a la imagen que pueda acordarse.

Así mismo, en el caso de que la videovigilancia sea necesaria para el control de la actividad laboral y de forma temporal por el conocimiento de la comisión de un ilícito laboral, deberá haberse determinado en el convenio colectivo correspondiente las circunstancias en que puede aceptarse, esta forma de control laboral, la duración que deberá ser siempre de carácter temporal y que en ningún caso se podrán aceptar como informaciones previas que exista un cartel informativo si el uso de dispositivos de videovigilancia se usa en otras instalaciones de la empresa por motivos de seguridad.

Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral

De la misma manera que en el artículo 89, en el 90 DEL LOPDGSS, se regula otra forma de control de los trabajadores: "los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización".

Pero a diferencia del art. 89, el 90 determina algunas diferencias en cuanto a cómo debe ser la información y añade algunos derechos de protección, no todos: con carácter previo, los empleadores habrán de informar de forma **expresa, clara e inequívoca** (**en la videovigilancia es expresa, clara y concisa**) 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. (**Los derechos son de supresión, oposición, portabilidad, limitación, acceso, y rectificación, -SOPLAR-, antes ARCO**).

Los sistemas de geolocalización con carácter general, pueden ser muy invasivos de los derechos fundamentales de los trabajadores, sobre todo en materia de tránsito, descansos, salud laboral, etc.

Un sistema de geolocalización permite un continuo y permanente seguimiento durante su uso, de una persona u objeto, y no sólo del posicionamiento de alguien, sino también del lugar exacto donde está esa persona, pudiendo hacerse un uso del tratamiento de los datos completamente distinto del anunciado, incluso pudiéndose extraer conclusiones del dispositivo de muy diferentes formas

y, sin una completa homologación o revisión de su actividad y de si funciona adecuadamente o no, aportándose como medio de prueba en sede judicial para demostrar por ejemplo, un pretendido incumplimiento contractual.

Pero no existe una regulación como sí existe de los tacógrafos en los autocares o autobuses, ni de los sistemas de radar que se utilizan para las infracciones en materia de tráfico, para avalar que funcionan correctamente y que no han sido manipulados, por lo que pueden llegar a ser de muy dudosa credibilidad.

Además, el derecho del afectado a ser informado de quién posee los datos personales y con qué fin, es muy importante en relación con estos sistemas, pues la libertad del individuo es la más afectada y las facultades empresariales de control, no deben ser tan extensas, porque se encuentran limitadas por otros derechos fundamentales.

Por supuesto, el interés privado del empresario no podrá justificar que el tratamiento de datos empleado en contra del trabajador pueda darse sin una información previa sobre el control laboral puesto en práctica, porque no hay en el ámbito laboral, una razón que tolere la limitación del derecho de información que integra la cobertura ordinaria del derecho fundamental del art. 18.4 CE.

Por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la ley o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; sino que el control empresarial por esa vía, aunque podrá producirse, deberá asegurar también la debida información previa.[37]

Y por supuesto si existen los derechos "Soplar" en el tratamiento, en general, de los datos de carácter personal, ¿cabría no establecer el derecho de oposición o revocación del consentimiento dado porque la ley, frente al RGPD lo haya limitado? Parece que no, lo que determinaría una clara contradicción de la LOPDGDD frente al RGPD, de nuevo.

La AEPD ha venido a establecer la siguiente información en relación con la determinación de los dispositivos de GPS para el control de la actividad de los trabajadores:

"Si usas el coche de tu empresa y han instalado un GPS con una finalidad de control, también han de informarte con carácter previo a su puesta en funcionamiento.

Los procedimientos de recogida de información pueden ser muy variados y, por tanto, los modos de informar a los interesados deben adaptarse a las

circunstancias de cada uno de los medios empleados para la recopilación o registro de los datos.

Por otra parte, las comunicaciones al interesado sobre datos ya disponibles, o tratamientos adicionales, pueden hacerse llegar, entre otros medios, por correo postal, mensajería electrónica, así como notificaciones emergentes en servicios y aplicaciones.

Las características de cada uno de los medios varían en cuanto a extensión, disponibilidad de espacio, legibilidad, posibilidad de vincular informaciones, etc. En cualquier caso, la información a las personas interesadas debe proporcionarse: con un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso.

Para facilitar este cumplimiento, se recomienda adoptar un modelo de información por capas o niveles, que consiste en lo siguiente:

En un primer nivel, presentar una información básica (identificación del responsable, finalidad del tratamiento, ejercicio de derechos, origen de los datos, realización de perfiles), de forma resumida, en el mismo momento y medio en que se recojan los datos.

En un segundo nivel, la información adicional, presentando de forma detallada el resto de informaciones (podría incluirse la política de privacidad).[38]

No cabe duda de que estos sistemas de control deben ser regulados y limitados en los convenios colectivos estableciendo reglas precisas y finalidades lícitas adecuadas que impidan la extralimitación de los empresarios a la hora de organizar la actividad laboral, y sobre todo utilizando medidas de carácter previo iniciales menos invasivas de los derechos fundamentales de los trabajadores.

Derechos digitales en la negociación colectiva

En el art. 91 se reconoce el derecho a que los convenios colectivos establezcan "garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral".

Es curioso como en este artículo, si se mencionan los convenios colectivos. Varias cuestiones se pueden llevar a la negociación colectiva además desde la formación de los trabajadores y trabajadoras en materia de protección de datos, a la formación a los representantes de los trabajadores, así como la ampliación de los derechos de información y consulta en materia "digital", o la prevención

de los riesgos derivados del uso de las nuevas tecnologías. El convenio colectivo tiene un papel importante en el avance de la protección de los derechos fundamentales y éste además será un derecho a tener muy en cuenta en la revolución 4.0.

Pero sobre todo es necesario regular como se va a actuar en relación en los distintos momentos de la relación de trabajo, en los que se recaban datos de carácter personal y que son:

1. En el acceso a los portales de empleo,
2. En los procesos de selección de personal,
3. En relación con el uso del correo electrónico,
4. En relación con el control del absentismo y los datos de salud de los trabajadores,
5. En relación con la prevención de riesgos laborales, y vigilancia de la salud,
6. En relación con los servicios de prevención de riesgos laborales,
7. En relación con el acceso a los datos por los delegados de prevención,
8. En relación con la Cesión de datos de trabajadores a contratistas

Entre otros, para lo que independientemente de la aplicación de los principios generales, y demás cuestiones contenidas en este documento con carácter general, la UGT, ha establecido un canal de asesoramiento que permitirá conocer la casuística que se está dando en las empresas y la posibilidad de asesorar a los representantes de los trabajador y trabajadoras y a los mismos en estas cuestiones.

Registro horario

El Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, incluye reformas normativas dirigidas a regular el registro de jornada, como forma de combatir la precariedad laboral.

Tal y como se señala en el mismo, "a pesar de que nuestro ordenamiento laboral, en línea con los ordenamientos europeos, se ha dotado de normas que permiten cierta flexibilidad horaria para adaptar las necesidades de la empresa a las de la producción y el mercado (distribución irregular de la jornada, jornada a turnos u horas extraordinarias), esta flexibilidad no se puede confundir con el incumplimiento de las normas sobre jornada máxima y horas extraordinarias."

La modificación del art. 34 del ET, añade un nuevo apartado 9, con la siguiente redacción: "La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo. Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de jornada. La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social".

En un momento inicial parece que la modificación de este artículo, su control no corresponderá también a la AEPD sin embargo no es así, puesto que cualquier forma de control de los trabajadores que implique el conocimiento, la captación y el tratamiento informático de datos de carácter personal, de nuevo hace que entren en funcionamiento las normas relativas a la protección de los mismos, y por lo tanto, sus principios y límites, luego teniendo en cuenta los principios anteriores y sobre todo el de minimización, dado que en el mercado existen numerosas formas de control horario sin afectar a los derechos a la intimidad, a la imagen, a la libertad de tránsito, etc. o que sí afecten. Es necesario ponderar al máximo los intereses en conflicto a la hora del uso de mecanismos y aparatos de control horario.

NOTAS

[1] Para UGT, el convenio colectivo sectorial estatal puede regular determinadas cuestiones en esta materia que unifiquen el tratamiento sectorial, independientemente de que el convenio de empresa o grupo de empresa será el ámbito natural.

[2] https://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf

[3] Convention for the protection of individuals with regard to the processing of personal data.

[4] Textos refundidos del Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950; el protocolo adicional al Convenio, hecho en París el 20 de marzo de 1952, y el protocolo número 6, relativo a la abolición de la pena de muerte, hecho en Estrasburgo el 28 de abril de 1983. BOE de 6 de mayo de 1999.

[5] El TS y el TC, por ejemplo, y en materia de uso de las nuevas tecnologías para el control de la actividad laboral, han venido abandonando el criterio de la proporcionalidad de la medida, para pasar a analizar los distintos supuestos del "control tecnológico" desde una posible expectativa de confidencialidad, teniendo en cuenta el deber de información previa al trabajador para legitimar el registro en el ordenador, los correos electrónicos, etc.

La STS (26 de septiembre de 2007) ya vino a señalar que: "lo que debe hacer la empresa según las exigencias de la buena fe, es fijar previamente las reglas de uso de los medios, con prohibiciones absolutas o parciales, e informar a los trabajadores de que va a existir un control de su trabajo y de los medios que han de aplicarse en orden a la comprobación de los mismos".

Las sentencias STC 241/2012 y STC 170/2013, construyeron la idea de que independientemente de las prohibiciones o no, con fines personales, de los instrumentos puestos a disposición del trabajador, tiene el derecho a una "expectativa general de confidencialidad" de sus usos privados y de sus comunicaciones.

La Sala 2ª del TS, en cambio, en su sentencia de 16 de junio de 2014 (Rec. 2229/2013) señaló que "es necesaria la autorización judicial para acceder a la cuenta de correo de un trabajador".

Aunque esta Sala 2ª deja fuera a las págs. web señalando que no forman parte de la comunicación propiamente dicha y no están por tanto protegidas por el secreto de las comunicaciones.

[6] El considerando 155, habla de que el Derecho de los Estados miembros o los convenios colectivos, incluidos los convenios de empresa, pueden hacerlo.

[7] Apartado segundo de la norma.

[8] Informes sobre datos de las mutuas y los servicios de prevención, acceso de los delegados de prevención en accidentes de trabajo, cesión de los datos de los trabajadores, sobre el art. 42 del ET, sobre el acceso a datos de prevención de riesgos laborales, sobre el acceso de datos en el caso de un despido utilizando un GPS, sobre el interés legítimo y la ponderación del mismo, etc.

[9] Que han servicio en parte, para la confección de este Protocolo.

[10] Dictamen 4/2007 sobre el concepto de datos personales adoptado el 20 de junio, Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas el 28 de noviembre de 2017, Dictamen 2/2017, sobre el tratamiento de datos en el trabajo, adoptado el 8 de junio de 2017, etc.

[11] Art. 4.1 RGPD lo define como toda información sobre una persona física identificada o identificable.

[12] Dictamen grupo de trabajo 4/2007.

[13] ¿Qué pasa con un comerciante que ha instalado un sistema de videovigilancia en su tienda y exhibe en ella imágenes de unos ladrones incluido el trabajador de la tienda? A pesar de que intervenga la policía y difumine los rostros de los presuntos ladrones, es posible que exista la posibilidad de que las personas que aparecen en las imágenes puedan ser reconocidas por sus amigos, parientes, o vecinos por lo que se podría vulnerar el derecho de protección de datos de todos los incluidos en la imagen.

[14] Dictamen 4/2007 sobre el concepto de datos personales.

[15] Ídem Dictamen 4/2007.

[16] STS de 18 de diciembre de 2006, Rec. núm. 112/2005

[17] En todo caso en relación con las encuestas estadísticas y la combinación de información dispersa, los estadísticos están sujetos a un deber específico de secreto profesional, por lo que no pueden publicar datos que no sean anónimos. Esta prohibición les obliga a publicar datos estadísticos agregados que no puedan atribuirse a una persona identificada (Ídem Dictamen 4/2007).

[18] AEPD: Informe 0154/2010

[19] Primera sentencia tras la LOPDGDD, dictada en el ámbito de la videovigilancia por el Juzgado de lo social 3 de Pamplona de 18 de febrero de 2019 proc. despido 875/2018.

[20] Dictamen 2/2017 sobre el tratamiento de datos en el trabajo adoptado el 8 de junio de 2017.

[21] Los principios de proporcionalidad y subsidiariedad harán que en ocasiones no se deben utilizar determinados tratamientos si hay otros menos invasivos del derecho fundamental de protección de datos y otros derechos conexos y unidos a él.

[22] De ahí que el convenio colectivo tenga un papel fundamental en la protección del derecho lo que se desarrollará en otro epígrafe.

[23] Dictamen grupo de trabajo 2/2017 y Dictamen 01/2017 sobre la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas (en inglés), WP 247 de 4 de abril de 2017, p. 29, http://ec.europa.eu/newsroom/document.cfm?doc_id=44103 (versión en inglés).

[24] No obstante, el responsable del tratamiento está exento de la obligación de comunicar información al interesado en los casos en los que el registro o la recopilación de datos estén expresamente prescritos por ley.

[25] Es difícil que sea una declaración verbal sin documentar, porque el RGPD exige la prueba del consentimiento.

[26] Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

[27] Estrictamente, es problable que se refiera al principio de minimización.

[28] Este extracto, aunque parezca resumido por interesado, viene a coincidir en cierta medida con todos los postulados anteriores pues son en el Reglamento y los documentos comunitarios en los que se han basado, y Sentencia del Juzg de lo Social de Pamplona antes referenciada.

[29] Para garantizar que el consentimiento se haya dado libremente, éste no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular.

Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando éste no sea necesario para dicho cumplimiento.

[30] https://www.aepd.es/media/guias/guia-listado-de-cumplimiento-del-rgpd.pdf

[31] Artículo 22. 3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

[32] Englobando los mismos derechos para los empleados públicos.

[33] Informe AEPD. https://www.aepd.es/media/informes/informe-juridico-rgpd-grabacion-de-imagenes-y-voz-proporcionalidad.pdf

[34] AEPD https://www.aepd.es/media/memorias/memoria-AEPD-2017.pdf

[35] Art. 13 RGPD: 1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

d) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

e) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

[36] Ficha práctica ejemplificativa sobre las cámaras para el control empresarial AEPD: https://www.aepd.es/media/fichas/ficha-videovigilancia-control-empresarial.pdf

[37] STSJ Andalucía (Granada) de 19 de octubre de 2017 Roj: STSJ AND 11675/2017- ECLI: ES:TSJAND:2017:11675

[38] https://www.aepd.es/media/guias/guia-ciudadano.pdf

Autora:
Susana Bravo Santamaría, *Abogada del Servicio de Estudios de la Confederación (UGT)*
Edita:
Comisión Ejecutiva Confederal de UGT
Avda. de América, 25. 28002 Madrid

Depósito Legal: M-17861-2019


UGT