PROTOCOLO DE ACTUACIÓN PARA LA NEGOCIACIÓN COLECTIVA

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

Presentación

La presente guía sindical es un instrumento de apoyo al "Protocolo de actuación para la negociación colectiva en materia de protección de datos de carácter personal y garantía de los derechos digitales" ya que permitirá conocer de una manera esquemática y rápida, en que consiste el derecho de protección de datos de carácter personal, y qué datos lo son y qué datos no lo son y cuándo el interés legítimo es digno de protección prioritariamente a la protección de los datos de carácter personal y cuando no, teniendo siempre presente, que corresponde a los trabajadores y trabajadoras la protección de sus datos de carácter personal, derecho a la protección de los mismos que tiene rango constitucional, afectando a otros derechos también constitucionales en determinadas ocasiones, como el derecho a la imagen, la libertad de tránsito, el derecho a la intimidad y a la vida privada, etc. Los empresarios deben tener un comportamiento muy cuidadoso a la hora de recoger y tratar tales datos, a la hora de controlar la organización del trabajo, con instrumentos que pretendan recabar datos de carácter personal y a la hora de limitar el desarrollo de la vida privada y social de los trabajadores en el centro de trabajo.


101000
011011

Introducción

La consulta de esta guía permitirá resolver algunas cuestiones de manera rápida e inmediata, sin embargo, por la importancia del derecho y la necesidad de regular en los convenios colectivos la defensa del derecho a la protección de datos de carácter personal, es importante tener a mano el libro titulado, como ya hemos señalado el: "Protocolo de actuación para la negociación colectiva en materia de protección de datos de carácter personal y garantía de los derechos digitales". Los representantes de los trabajadores y los sindicatos, tenemos un papel fundamental en la defensa de los derechos fundamentales en el ámbito del trabajo, y la organización del mismo por parte de los empresarios no debe ser un límite al ejercicio de tales derechos, por lo que no solo los trabajadores tienen la obligación de proteger este especial derecho fundamental, sino también nosotros, los sindicatos y los representantes de los trabajadores en todos los ámbitos, tanto a nivel sectorial estatal, como a nivel de empresa, tenemos la obligación de estar al lado de los trabajadores y trabajadoras para su protección, y llevar a los convenios colectivos la regulación de cuantas cuestiones sean necesarias para la protección del derecho.

¿QUÉ SON LOS DATOS DE CARÁCTER PERSONAL?

Los datos de carácter personal, son todos aquellos, que identifican a una persona directamente, o indirectamente la hacen identificable.

Cualquier dato , 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. 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.

Ejemplos de cómo puede ser identificable una persona

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.

- 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,

- el DNI electrónico tiene datos biométricos, por lo que no debe utilizarse como método de control de los trabajadores.
  - Los datos estadísticos son datos personales en ocasiones.
- en el caso de cesión de los datos de los trabajadores, la misma únicamente podría entenderse amparada en caso de que se produjera en el ámbito de las funciones desarrolladas por los Delegados de Personal o el Comité de Empresa, al encontrarse reconocido por el Estatuto de los Trabajadores (ET), el derecho de los representantes de los trabajadores, que lo está en el art. 64 ET, a acceder a determinados datos de los trabajadores en el ámbito de sus competencias. Informe AEPD 154/2010
- 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.

¿POR QUÉ HAY QUE PROTEGERLOS Y QUIÉN DEBE HACERLO?

El derecho fundamental a la protección de datos de carácter personal está en el art. 18.4 de nuestra Constitución obligando a que la ley limite el uso de la informática para garantizar la intimidad personal y familiar de los ciudadanos, el honor, el derecho de imagen, la libertad de circulación, el secreto de las comunicaciones y otros derechos y libertades que pueden verse afectados, y la legislación europea y española, reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos, e incluso a que los convenios colectivos regulen esta materia para la protección de todos los derechos en conflicto.

Corresponde a cada trabajador y trabajadora en cuanto tal, y en las relaciones de trabajo, la protección de sus datos de carácter personal y la defensa de los mismos, defensa que también puede articularse a través de los representantes de los trabajadores y los sindicatos, y regularse en el convenio colectivo como ya hemos dicho, independientemente del derecho de consulta que, sobre determinadas cuestiones, en esta materia, tienen tales representantes de los trabajadores.

¿CUÁLES SON NUESTROS DERECHOS COMO TRABAJADORES Y TRABAJADORAS?

Si cualquier trabajador como consecuencia de una obligación legal o por otros motivos debe proporcionar datos de carácter personal, tiene el derecho a tener la información previa y adecuada y por capas, es decir, para cada una de las finalidades para la que se recaben los datos, con el objeto de proteger y controlar los mismos, es decir, para saber, para qué se recogen, dónde están y como se están protegiendo por los responsables de su protección, etc. Porque no se pueden obtener datos de los trabajadores y trabajadoras de forma desconocida, oculta, ilícita, ilegal, etc….

Sobre todo en el ámbito laboral, no se pueden obtener datos sin información previa de para que se necesitan, tanto si es como consecuencia de la aplicación de una ley como si no, y sin una necesidad legal, sin una finalidad o un interés legítimo, sin un motivo o causa, porque además pueden existir otros derechos fundamentales que pueden verse afectados, de ahí que los datos que se recaben no pueden ser excesivos y debe afectar lo menos posible a la esfera de la intimidad de las personas trabajadoras (principio de minimización).

El derecho de información previa la base de todo:

- La obligación de información previa de los empresarios y el correlativo derechos de los trabajadores y trabajadoras, debe contener: el porqué de la recogida de los datos, tanto si la base es de carácter legal, por ejemplo,

para formalizar el contrato de trabajo como si no, para dar cumplimiento a las obligaciones en materia de Seguridad Social y de carácter fiscal o tributario, etc.

- El derecho a la información, exige que se comuniquen, por tanto, los fines para los que se recogen los datos, sean cual sea la base de la recogida, legal o de otro tipo, y que las necesidades sean explícitas, adecuadas, exactas, y limitadas a lo necesario.

- Pero también deben estar actualizados y solo se pueden mantener o guardar un tiempo limitado, es decir no más tiempo del necesario, y sobre todo, si se ha pedido la cancelación de los mismos, no pueden seguir tratándose, solo en determinadas ocasiones pueden guardarse más tiempo, por ejemplo para el cumplimiento de una obligación legal, pero si se ha manifestado la oposición o cancelación de la persona trabajadora, solo los realmente necesario en virtud de dicha información legal, deben mantenerse.

Derechos SOPLAR, ya no ARCO

Los derechos de supresión, oposición, portabilidad, limitación, acceso, rectificación, permiten a los titulares de los datos, que no se recaben datos excesivos, o se limite su recogida, o puedan rectificarlos u oponerse a los que se pretendan recoger, o incluso modificar el consentimiento recabado, derechos que se ejercen igualmente en el ámbito laboral.

¿CUÁLES SON LOS FUNDAMENTOS DE LA RECOGIDA DE DATOS DE CARÁCTER PERSONAL Y SU TRATAMIENTO O ALMACENAMIENTO INFORMÁTICO O NO INFORMÁTICO?

Para que los datos que se recogen se puedan almacenar tiene que darse al menos una de las siguientes condiciones:

- Que se necesiten para la ejecución de un contrato, en este caso de trabajo o un precontrato laboral.
- Para proteger intereses vitales del titular o de otra persona.
- Para el cumplimiento de obligaciones de interés público o del ejercicio de poderes públicos.
- Para la satisfacción de intereses legítimos propios, o de un tercero, siempre que sobre dichos interese no prevalezcan los intereses o los derechos y libertades fundamentales del titular de los datos personales que requieran su protección.
- Cuando se dio el consentimiento para el tratamiento de los datos. Sin embargo, el consentimiento en el ámbito laboral tiene una consideración especial y no vale de cualquier manera.

El consentimiento en el ámbito laboral

En materia de protección de datos, en el ámbito del trabajo, la base para obtener datos de carácter personal NO

PUEDE SER EL CONSENTIMIENTO. Pese a la propia dicción del Reglamento, este consentimiento ha sido matizado por las instancias europeas. Esto es así por la especial naturaleza de la relación entre el empresario y el trabajador. Además, el órgano europeo denominado "Grupo de trabajo del artículo 29, en la actualidad Comité de protección de datos", ha determinado que efectivamente el consentimiento en el ámbito laboral, solo es válido, si la negativa a otorgar el mismo, **no supone la posibilidad de que el trabajador vaya a ser represaliado por la misma**.

Hay que tener en cuenta que el consentimiento del trabajador puede ser revocado por el mismo en cualquier momento.

En todo caso para que el consentimiento pueda otorgarse válidamente debe tenerse en cuenta:

- La información previa y por capas, es decir, tanto si hay una base legal, como un interés legítimo, como cualquier otra cuestión que determine la necesidad de solicitarlo, debe existir previamente dicha información previa, y para que finalidad se recaba.
- Debe ser afirmativo, claro, que se refleje como una manifestación de voluntad libre, específica, informada, e inequívoca del trabajador o trabajadora, de que da sus datos libremente y acepta el tratamiento de datos de carácter personal que le conciernen.

Como el empresario en su caso debe acreditar que el consentimiento ha sido obtenido válidamente, este debe constar:

- Por escrito, aunque se puede dar de forma verbal, si luego se puede acreditar tal circunstancia,
- Por medios electrónicos,
- Pero siempre debe poder ser revocable.

Por todo lo anterior, la configuración por defecto en los dispositivos digitales, o la instalación de programas informáticos que faciliten 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.

El Interés legítimo

Otra posibilidad para solicitar u obtener datos de carácter personal y tratarlos informáticamente o almacenarlos es el interés legítimo de los empresarios. ¿Qué es el interés legítimo?

El interés legítimo significa que el empresario puede necesitar obtener y almacenar o tratar, determinados datos de los trabajadores para preservar bienes o derechos. Pero su interés de protección de dichos bienes o derechos o incluso el control de la actividad laboral no es legal, sino se tienen en cuenta:

La regla de la ponderación: para que sea válido el interés legítimo del empresario debe aplicarse la regla de la ponderación, lo que significa que entre dicho interés legítimo y los derechos fundamentales de los afectados solo será válida la aplicación de dicho interés sino prevalecen los derechos fundamentales de los afectados.

La regla de la ponderación debe realizarse como un examen previo a cada caso concreto de pretensión de acudir al interés legítimo empresarial, para recabar datos de carácter personal de los trabajadores de cualquier forma (dados por los mismos u obtenidos por medio de aparatos tecnológicos), porque será necesario valorar si en el supuesto concreto de que se trate, existirá un interés legítimo perseguido por el responsable del tratamiento o por un tercero o terceros a los que se comuniquen los datos, que prevalezca sobre los derechos y libertades fundamentales del trabajador o trabajadora y que requieran protección conforme a lo dispuesto en el artículo 1 del RGPD, o si, por el contrario, los derechos fundamentales o intereses de las personas trabajadoras a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo de los anteriores.

¿QUÉ PUEDEN HACER LOS SINDICATOS Y LOS REPRESENTANTES DE LOS TRABAJADORES POR LA PROTECCIÓN DE NUESTROS DATOS DE CARÁCTER PERSONAL?

- Exigir a las empresas la revisión de los documentos que pretendan darse a los trabajadores y trabajadoras,
- Tener información precisa y detallada de los fundamentos, interés legítimo, finalidad, análisis de la ponderación de los derechos afectados y la aplicación del principio de minimización para recabar los datos de carácter personal en todos los ámbitos de las relaciones laborales.
- No permitir recabar el consentimiento de los trabajadores y trabajadoras sino es posible negarse a darlo sin consecuencias negativas para los mismos.
- Negociar en los convenios colectivos en todos los ámbitos la protección del derecho, el derecho de información y consulta, y ampliar los márgenes del art. 64 del ET, independientemente de los datos a los que se puede tener acceso en virtud del RD6/2019, de 1 de marzo, de medidas urgentes para garantía de la igualdad de trato y de oportunidades entre mujeres y hombres en el empleo y la ocupación.
- Asesorar a los trabajadores y trabajadoras en caso de vulneración del derecho de protección de datos y otros posibles derechos implicados de los mecanismos judiciales y administrativos existentes: la jurisdicción so-

cial, y la Inspección de Trabajo y Seguridad Social (ITSS) y la Agencia Española de Protección de Datos (AEPD).A nivel confederal, el Servicio de Estudios de la Confederación dará respuesta a cuantas dudas puedan plantearse, y ejercitará las actuaciones correspondientes ante los órganos europeos en caso necesario.

¿LAS EMPRESAS PUEDEN DAR DATOS A LOS REPRESENTANTES DE LOS TRABAJADORES, A LOS SINDICATOS Y A LOS DELEGADOS DE PREVENCIÓN DE RIESGOS LABORALES, ETC.?

Por supuesto, todos aquellos datos que se encuentren dentro de las competencias establecidas en el art. 64 del ET, así como en materia de Seguridad y Salud y en determinados supuestos de vigilancia de la Salud, como por ejemplo, los datos que se dan a los delegados de prevención de riesgos laborales en relación con las conclusiones que se deriven de los reconocimientos efectuados relativos a la aptitud del trabajador para el desempeño del puesto de trabajo o la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva, son datos que tienen una base legal y necesaria y deben ser dados a las respectivas representaciones de los trabajadores.

Igualmente, en relación con el reciente Real Decreto 6/2019, de 1 de marzo, de medidas urgentes para garantía de la igualdad de trato y de oportunidades entre mujeres y hombres en el empleo y la ocupación, determinados datos necesarios en relación con las auditorías salariales, así como los relativos para realizar el diagnóstico negociado en materia de igualdad y en relación con el:

a) Proceso de selección y contratación.

b) Clasificación profesional.

c) Formación.

d) Promoción profesional.

e) Condiciones de trabajo, incluida la auditoría salarial entre mujeres y hombres.

f) Ejercicio corresponsable de los derechos de la vida personal, familiar y laboral.

g) Infrarrepresentación femenina.

h) Retribuciones.

i) Prevención del acoso sexual y por razón de sexo, deben darse por las empresas, para realizar el correspondiente Plan de igualdad.

El empresario también con esta nueva regulación, está obligado a llevar un registro con los valores medios de los salarios, los complementos salariales y las percepciones extrasalariales de su plantilla, desagregados por sexo y distribuidos por grupos profesionales, categorías profesionales o puestos de trabajo iguales o de igual valor. Las personas trabajadoras tienen derecho a acceder, a través de la representación legal de los trabajadores en la empresa, al registro salarial de su empresa.

En relación con el registro de jornada, de la misma manera, 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 ha venido a establecer la obligatoriedad del registro diario de jorna-

da, y será: “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, que se organizará y documentará este registro de jornada.

Por lo tanto, de la misma manera para la utilización de cualesquiera instrumentos o aparatos que pretendan registrar la jornada de los trabajadores, se deberá tener en cuenta lo anterior además de los principios del RGPD y de la LOPGDD, cuando dichos instrumentos recojan y traten datos de carácter personal de los trabajadores y trabajadoras.

GARANTÍA DE LOS DERECHOS DIGITALES

¿Qué son los derechos digitales?

El legislador español a la hora de regular determinadas cuestiones en materia de protección de datos, teniendo siempre en cuenta que, en caso de contradicción, el Reglamento europeo es la norma que tiene la última palabra, o el máximo intérprete europeo: el Tribunal de Justicia de la Unión Europea (TJUE), inclusive el TEDH, no ha determinado con claridad que debe entenderse por derechos digitales. Por eso tal y como señala el Reglamento europeo, los convenios colectivos tienen un papel muy importante en esta materia.

Derecho a la intimidad y uso de dispositivos digitales

En todas estas materias en las que los convenios colectivos podrán establecer regulaciones adecuadas para la protección del derecho de las personas trabajadoras a la protección de sus datos de carácter personal, puesto que los dispositivos digitales utilizan números datos que pueden hacer identificable a cualquier trabajador o trabajadora, es necesario:

- Un convenio colectivo, cualquier determinación relativa a los dispositivos digitales puestos a disposición de los trabajadores, debería tener la cobertura de una norma convencional, para evitar la limitación del uso particular de los dispositivos digitales, dada la necesi-

dad de "vida social laboral" de los trabajadores, con carácter global.

- Se pueden establecer limitaciones temporales en dicho uso y para fines privados por ejemplo, para evitar la competencia desleal a la empresa o para limitar el ejercicio de funciones relativas a otros trabajos que pudieran ser objeto de pluriempleo por parte del trabajador, pero siempre por convenio colectivo.

- 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.

- Se puede establecer en el convenio que, 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 mediante los dispositivos digitales a las trabajadoras y trabajadores, con instrumentos como GPS, IP del te-

léfono o el ordenador, videovigilancia, huella dactilar, iris del ojo, datos biométricos en general, etc. teniendo en cuenta los anteriores como último recurso y en aplicación del principio de minimización, porque en otro caso, la protección de los derechos en conflicto es motivo de demanda ante la jurisdicción social y sanciones por parte de la AEPD y la ITSS.

- 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, y su concreción en los convenios de empresa en su caso.

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 LOPD-GDD, 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 siempre 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

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 com-

plementarias en el correspondiente contrato a tiempo parcial, o de los tiempos de presencia, tiempos a disposición del empresario, etc., lo que también 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 suficientes 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?

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".

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 trabajado-

res 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.

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 limites 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.

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.

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.

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

En resumen los sistemas de videovigilancia para el control empresarial solo deberían adoptarse cuando exista una relación de proporcionalidad entre la finalidad perseguida y el modo en que se traten las imágenes, y no haya otra medida más idónea, el 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.

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 esta-

blecen 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.

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 permita la limitación del derecho de información que integra la cobertura ordinaria del derecho fundamental del art. 18.4 CE.

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".

La regulación de la utilización del GPS, debe hacerse también en el convenio colectivo, porque en base al principio de minimización puede vulnerar numerosos derechos. Por supuesto su regulación debe contemplar que deje de funcionar, sí se instala en un medio de transporte de la empresa o en el móvil de la empresa a disposición del trabajador, terminada la jornada laboral y sin que sea el trabajador o trabajadora el que tenga que realizar funciones de desconexión y mantenimiento, porque serían obligaciones añadidas ajenas a las funciones del grupo profesional que no competen al mismo y se estaría extralimitando la empresa en mandatarlas.

Para facilitar este cumplimiento, se recomienda adoptar un modelo de información por capas o niveles.

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

Varias cuestiones se pueden llevar a la negociación colectiva, 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 los distintos momentos de la relación de trabajo, en los que se recaben 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 e instrumentos digitales

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: "9. 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 mi-

nimización, 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, y a la utilización de datos incluso biométricos es necesario ponderar al máximo los intereses en conflicto, a la hora del uso de mecanismos y aparatos de control horario.

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-17862-2019


UGT