

LA PROTECCIÓN DE DATOS PERSONALES DE LOS EMPLEADOS EN EL REGISTRO DE LA JORNADA Y LOS DENOMINADOS “DERECHOS DIGITALES”

The protection of employees personal data in the daily log
and so-called "digital rights"

JOSÉ ANTONIO MARCOS HERRERO

Abogado. Ilustre Colegio de Abogados de Málaga

Fecha de recepción: 31/06/2019

Fecha de aceptación: 04/07/2019

SUMARIO: 1. EL ARTÍCULO 34 DEL ESTATUTO DE LOS TRABAJADORES Y LA OBLIGACIÓN DEL EMPLEADOR DE IMPLANTAR UN REGISTRO DIARIO DE LA JORNADA. 2. LA APLICACIÓN DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN LA IMPLANTACIÓN DEL REGISTRO DE LA JORNADA. 2.1. Obligaciones del responsable en el tratamiento de los datos personales de los empleados para el control diario de la jornada. 2.2. Implantación de dispositivos para el control diario de la jornada que tratan datos biométricos de los empleados. 3. LOS DENOMINADOS “*DERECHOS DIGITALES*” EN LA NUEVA LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTÍA DE DERECHOS DIGITALES. *LA DESCONEXIÓN DIGITAL* Y OTROS DERECHOS DE APLICACIÓN EN EL ÁMBITO LABORAL. 4. CONCLUSIONES.

RESUMEN: La obligada implantación del registro diario de la jornada supone también la necesidad de las empresas de cumplir con las exigencias derivadas del Reglamento General de Protección de Datos, con ocasión del tratamiento de los datos personales de los empleados. Igualmente la nueva Ley Orgánica de Protección de Datos, que añade a su

regulación la novedosa garantía de los “derechos digitales”, incorpora una serie de derechos de los trabajadores en el ámbito de la sociedad digital, destacando el “derecho a la desconexión digital en el ámbito laboral”, que obliga al empleador a hacer efectivo este nuevo derecho.

ABSTRACT: The mandatory implementation of the daily log also implies the need for companies to comply with the requirements of the General Data Protection Regulation (GDPR), in relation to the processing of employees personal data. Likewise, the new Organic Act on Data Protection, introduces the new guarantee called ‘digital rights’, it incorporates a number of rights for workers in the field of the digital society, highlighting the ‘digital right to disconnect in the workplace’, which mandates the employer to implement this new law.

PALABRAS CLAVE: Registro diario de la jornada, protección de datos personales, datos biométricos, derechos digitales, desconexión digital.

KEYWORDS: Daily log, protection of personal data, biometric data, digital rights, digital disconnection.

1. EL ARTÍCULO 34 DEL ESTATUTO DE LOS TRABAJADORES Y LA OBLIGACIÓN DEL EMPLEADOR DE IMPLANTAR UN REGISTRO DIARIO DE LA JORNADA

El artículo 10 del “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”, que regula el registro de la jornada laboral, modifica el apartado 7 del Artículo 34 de la Ley del Estatuto de los Trabajadores (ET) (Real Decreto Legislativo 2/2015, de 23 de octubre) y añade un nuevo apartado 9 al citado artículo 34, con el objetivo de crear un marco de seguridad jurídica, tanto para los empleados como para las empresas, facilitando la resolución de discrepancias en cuanto a la jornada laboral y, en consecuencia, sobre el salario. Con este articulado se sientan las bases para combatir la precariedad de las relaciones laborales, reconociendo el papel de la negociación colectiva.

Este registro de la jornada laboral supone una obligación para las empresas, que deben garantizar que se incluya el horario de inicio y finalización de la jornada de trabajo de cada trabajador. Para ello, la norma no se pronuncia sobre la forma en la que la empresa tiene que implantarlo, pudiendo por ello articular los instrumentos y procedimientos que entienda pertinentes. Es importante el papel que se le otorga a la parte social, pues la organización del sistema de control que se adopte debe ser fruto de la negociación colectiva, o en su defecto, de la decisión unilateral de la empresa tras la consulta a los representantes de los trabajadores (si existieran).

Un ejemplo de esta participación de los representantes de los trabajadores en la organización del registro, es el acuerdo suscrito (“instrucciones sobre el registro diario de jornada en Telefónica”), en fecha de 17 de Julio de 2019, entre la entidad Telefónica y los sindicatos UGT y CCOO en relación al registro diario de la jornada. Este documento viene a implementar determinadas directrices, de conformidad con la exigencia legal establecida en el artículo 34.9 ET, optando porque los trabajadores fichen a través de su Tarjeta de Identificación Personal (TIP) cuando acceden al centro de trabajo. Si los empleados no prestan sus servicios físicamente en el centro de trabajo (p.ej. teletrabajo), la entidad se compromete a la implementación de un sistema de registro telemático mediante el cual la persona trabajadora procedería al registro diario de su jornada

(el cual no implicará necesariamente la geolocalización). En todo caso, el acuerdo se compromete al cumplimiento de la normativa en protección de datos y respeto al art. 20 bis ET.

Para el cumplimiento de la obligación de registro de la jornada del art. 34 ET será válido “cualquier sistema o medio, en soporte papel o telemático”, debiendo documentarse la información de la jornada “en algún tipo de instrumento escrito o digital, o sistemas mixtos, en su caso, que garanticen la trazabilidad y rastreo fidedigno e invariable de la jornada diaria una vez registrada”. La posibilidad de utilización de diferentes sistemas para implantar el control horario nos conecta directamente con las cuestiones que vamos a tratar posteriormente. Si bien existen dificultades por parte del empleador en la aplicación de la norma, siendo criticada por su ambigüedad, se ha facilitado por el *Ministerio de Trabajo, Migraciones y Seguridad Social* una *Guía sobre el Registro de Jornada* en la que se recogen criterios, a título informativo, en relación con este deber formal empresarial, sin perjuicio de la interpretación de la norma que corresponde a los Juzgados y Tribunales del orden social. De igual forma, la Inspección de Trabajo y Seguridad Social (ITSS) aclara e interpreta los términos de la misma a través del “criterio técnico 101/2019 sobre actuación de la Inspección de Trabajo y Seguridad Social en materia de registro de jornada” (publicado en fecha el 10 de junio de 2019) ¹ que tiene por objeto el fijar criterios para la realización de las actuaciones inspectoras que se realicen a partir de la entrada en vigor del Real Decreto-ley 8/2019, de 8 de marzo, en relación con las disposiciones relativas al registro de jornada (art. 34.9 ET).

Es a partir del día 12 de mayo de 2019 desde cuando todas las empresas que tengan empleados tienen la obligación de garantizar un registro diario de la jornada.² Esta obligación debe incorporar la hora de inicio y de finalización de la jornada y, en relación con las interrupciones o pausas, la inspección de trabajo determina que el registro que se utilice debe ofrecer una visión adecuada y completa del tiempo de trabajo efectivo, por lo que el sistema implantado ha de ser “objetivo y fiable”. Sería conveniente que el empresario registrara este tipo de pausas, porque en caso contrario podría presumirse que la jornada laboral efectiva es toda aquella que transcurre entre la hora de inicio y finalización de la jornada de trabajo registrada.

El registro de la jornada no constituye un fin en sí mismo, sino un instrumento para el control del cumplimiento de la normativa en materia de tiempo de trabajo, con sus consecuencias respecto de la salud laboral, e implicaciones en la realización, abono y cotización

.....

1 Criterio que deja sin efecto la Instrucción 1/2017, complementaria a la Instrucción 3/2016.

2 La llevanza del registro de jornada no es una opción para el empresario, sino que se trata de un deber que deriva del término “garantizará” (Criterio ITSS 111/2019).

de las horas extraordinarias (siendo un medio que garantiza y facilita dicho control, pero no el único).

¿Qué consecuencias legales tiene para el empleador no garantizar el registro diario de la jornada? El empleador puede ser sujeto responsable de una infracción según el artículo 7 (apartado 5) del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que aprobó el Texto Refundido de la Ley sobre Infracciones y Sanciones en el Orden Social³ (LISOS), al disponer que es infracción grave la transgresión de las normas y los límites legales o pactados en materia de registro de jornada que se refiere en el artículo 34 del Estatuto de los Trabajadores. Si bien, según el criterio técnico 101/2019 ITSS, si hubiese certeza de que se cumple la normativa en materia de tiempo de trabajo o de que no se realizan horas extraordinarias, aunque no se lleve a cabo el registro de la jornada de trabajo, la valoración del inspector actuante en cada caso podría sustituir el inicio del procedimiento sancionador por la formulación de un requerimiento para que se dé cumplimiento a la obligación legal de garantizar el registro diario de la jornada de trabajo.

La inexistencia de este registro puede suponer para la empresa, igualmente, un déficit probatorio en la defensa de reclamaciones planteadas por sus empleados por la realización de horas extraordinarias, independientemente que se trate de un trabajador presencial o un teletrabajador (STSJ de Castilla y León - Sala Social - de 3 de febrero de 2016⁴), si bien para que proceda la inversión de la carga de la prueba, según dispone la STSJ de Castilla y León de 9 de junio de 2017 (Recurso 765/2017) es preciso que existan, cuando menos, indicios de que el trabajador pudiera hacer el horario que afirma realizar, y no basta con que se acredite la falta de registro y que el trabajador alegue la realización de horas extraordinarias, sino que ha de presentarse un panorama indiciario suficiente de la realización de excesos de jornada que permitan una mínima cuantificación.

Por el contrario, el cumplimiento de la implantación del sistema control horario del trabajador puede dotar a la empresa de la herramienta necesaria para justificar el descuento de la nómina mensual, ante el retraso injustificado del trabajador en la incorporación al puesto de trabajo (retraso en el fichaje de entrada) (STAN nº 82/2019 (Sala de lo Social), de 20 Jun. 2019, Rec. 115/2019).



3 Modificado por el Artículo 11 del Decreto-Ley 8/2019, de 8 de marzo.

4 La sentencia ratifica la condena a la empresa al pago de horas extraordinarias sobre la base de la inexistencia de control alguno sobre la jornada a pesar de tratarse de teletrabajo. No se admiten los argumentos de la empresa contra la reclamación de horas extraordinarias, alegando que al tratarse de una prestación de servicios con conexión remota y desde el domicilio del trabajador no se implementó control ni registro alguno para no interferir sobre el Derecho Fundamental a la intimidad e inviolabilidad del domicilio del empleado. Bien al contrario, ha de ser la propia empresa la que debe establecer las reglas de juego del control sobre el trabajador, sea un trabajador presencial o un teletrabajador, de modo que la ausencia de estos controles, y específicamente los de jornada, actúan en perjuicio claro de la empresa.

2. LA APLICACIÓN DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN LA IMPLANTACIÓN DEL REGISTRO DE LA JORNADA

Con la aprobación del 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 (Reglamento General de Datos Personales (en adelante, RGPD) se ha optado por una norma directamente aplicable en todos los estados de la Unión Europea, configurando un régimen común en todos ellos en el sistema de garantías, en el modelo de cumplimiento y en el modelo de supervisión en su aplicación por parte de las autoridades de control.

Es a partir de la entrada en vigor del RGPD, el 25 de Mayo de 2018, desde cuando cualquier tipo de organización, ya sea una gran empresa o “pyme”, debe evaluar su situación y adecuarse a los postulados de la norma⁵. Para ello debe realizar una adecuación de sus procedimientos internos, clausulado, y la adopción de las medidas técnicas y organizativas necesarias para adaptarse a los requerimientos establecidos en el RGPD. El empresario deberá poner en marcha las actuaciones necesarias para adaptarse a la norma y se pueda demostrar ante terceros su cumplimiento, aplicando las medidas de responsabilidad proactiva. Dentro de las medidas en las que se materializa este principio de responsabilidad proactiva del RGPD destacar “la figura del delegado de protección de datos, el registro de actividades de tratamiento, la protección de datos desde el diseño y por defecto, el análisis de riesgos y adopción de medidas de seguridad, la notificación de quebras de seguridad, las evaluaciones de impacto sobre la protección de datos, y la adhesión a códigos de conducta, mecanismos de certificación, sellos y marcas de protección de datos”.

Esta es una de las novedades que recoge el RGPD en relación a la normativa anterior, la aplicación del denominado principio de “responsabilidad proactiva” o *accountability*, por el que el “responsable del tratamiento”⁶ (que en este artículo será la empresa) debe aplicar las medidas necesarias a fin de garantizar que el tratamiento de los datos es conforme con la norma, y además ser capaz de demostrar ante los interesados⁷ y ante las autoridades de control (en España, la Agencia Española de Protección de Datos (AEPD) o autoridades

.....

5 Instituto Nacional de Ciberseguridad <https://www.incibe.es/protege-tu-empresa/blog/puntos-clave-adequacion-del-rgpd>).

6 Responsable del tratamiento (o responsable) es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros (Art. 4º.7 RGPD).

7 Personas físicas titulares de los datos, que sean objeto del tratamiento.

autonómicas competentes⁸) que ha adoptado las garantías adecuadas, y rendir cuentas por lo realizado.

El nuevo modelo de cumplimiento del RGPD se caracteriza porque es dinámico, no estático, por lo que se requiere a la empresa responsable una revisión permanente del cumplimiento de las garantías sobre los datos personales. En este marco, la empresa deberá acomodar su organización empresarial a las nuevas exigencias del RGPD.

En España, con la entrada en vigor el día 6 de diciembre de 2018 de la Ley Orgánica 5/2018 de 5 de diciembre, de protección de datos de carácter personal y garantía de los derechos digitales (en adelante, LOPDGDD), se incorporan nuevas obligaciones a las recogidas en el RGPD, o se amplían las ya previstas.

En relación a la protección de datos en el ámbito laboral, se podrán establecer normas específicas al respecto a través de leyes nacionales, convenios colectivos, convenios de empresa, etc.⁹, abriendo así la posibilidad de que las propias empresas elaboren normas internas para el tratamiento de datos personales de sus trabajadores. El empleador no solo deberá conocer las obligaciones que se establezcan en el RGPD y LOPDGDD, sino que deberá garantizar aquellas otras que se incorporen y sean objeto de desarrollo en el convenio colectivo, o acuerdo con los representantes de los trabajadores.

Por ello, si bien las empresas tienen la obligación de garantizar el registro diario de la jornada laboral, también deben adecuarse a los requerimientos exigidos por el RGPD en la implantación del citado registro, pues supone el tratamiento por el empleador de datos personales de sus empleados. El artículo 4.1 del RGPD ¹⁰define los “datos personales” como “toda información sobre una persona física identificada o identificable”, incluyendo en esta definición nuevas formas de identificar a una persona debido a los avances tecnológicos y su aplicación en el entorno empresarial. El Art. 9 RGPD igualmente regula el tratamiento de las denominadas “*categorías especiales de datos*”, e incorpora dos nuevas categorías en relación a las establecidas en la Directiva 95/46¹¹: los “datos genéticos” y los “datos biométricos dirigidos a identificar de manera unívoca a una persona física”.

.....

8 En el RGPD se establece que en cada estado miembro puede haber varias autoridades de control. En España, actualmente, además de la Agencia Española de Protección de Datos (AEPD), existen tres autoridades autonómicas con competencia en materia de protección de datos: *Autoridad Catalana de Protección de Datos*, regulada por la Ley 32/2010, de 1 de octubre; *Agencia Vasca de Protección de Datos* regulada por la Ley 2/2004, de 25 de febrero; y *el Consejo de Transparencia y Protección de Datos de Andalucía* regulado por la Ley 1/2014, de 24 de junio (si bien esta última aún no ha asumido materialmente la competencia ejecutiva sobre protección de datos personales, por lo que continuarán siendo ejercidas por la Agencia Española de Protección de Datos).

9 Considerando 155 y Art. 88 RGPD.

10 Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (Art. 4.1 RGPD).

11 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

El registro diario de la jornada supone la recogida y el tratamiento de datos personales de los empleados, que implica el control y monitorización diaria de las horas trabajadas por los empleados (horas de entrada y salida de los mismos), según el sistema implantado para la recogida de los mismos (aplicación que recoja las huellas dactilares de los trabajadores, su localización...).

Por ello, desde la publicación en el BOE del Real Decreto-ley 8/2019 el empleador, previamente a la implantación del registro, ha debido analizar los requerimientos legales exigidos al respecto en materia de protección de datos y haber valorado el sistema o mecanismo de registro a utilizar que sea más proporcionado. Es recomendable que la empresa cuente para ello con el asesoramiento de personal con conocimientos especializados en protección de datos y privacidad - como el delegado de protección de datos (DPD)¹²¹³-, ante la especial complejidad de la norma, debiendo participar en todas las cuestiones relativas a la protección de los datos de la organización desde la etapa más temprana posible. Este personal experto ayudará a la dirección de la empresa a adoptar medidas que sean proactivas, y también aquellas otras preventivas que identifiquen los riesgos ¹⁴ antes de que se materialicen, para así tomar las precauciones adecuadas para evitarlos o, por lo menos, mitigarlos.

El RGPD considera la figura del DPD como un elemento clave en el nuevo sistema de gestión de los datos, aportando una estimable ayuda a la empresa para cumplir con la norma, y con su tarea de asesorar, informar, formar, ser interlocutor y colaborar con la autoridad de control. Si bien en determinados supuestos es obligatorio que las empresas cuenten con un DPD, las organizaciones pueden considerar de utilidad nombrarlo de forma voluntaria.

El RGPD establece un catálogo de obligaciones que se imponen al responsable de tratamiento, y que vienen respaldadas por su régimen sancionador, de forma que el no cumplimiento de las distintas obligaciones que conllevan puede conducir a medidas correctivas.

2.1. Obligaciones del responsable en el tratamiento de los datos personales de los empleados para el control diario de la jornada

Al aportar el trabajador sus datos personales a la empresa, bien sea para formalizar el contrato laboral o posteriormente para la implantación del registro diario de la jornada, la empresa deberá informar al trabajador en los términos indicados en la norma ¹⁵ acerca de quién tratará sus datos personales, para qué finalidad o finalidades, los derechos que

12 Artículo 37.1 RGPD y 34.1 LOPDGDD.

13 Data Protection Officer (DPO).

14 El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento (art. 39.2 RGPD).

15 Art. 13 RGPD.

puede ejercer.... Este es el derecho de información que le asiste al trabajador por el tratamiento de sus datos personales, permitiendo la LOPDGDD (como novedad) que esa información se lleve a cabo “por capas”; es decir, el empleador facilitará al trabajador una información básica (al menos la identidad del responsable del tratamiento y de su representante, la finalidad del tratamiento y la posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 RGPD), indicándole igualmente una dirección electrónica u otro medio para que pueda conocer el resto de la información que tiene que ser suministrada por el responsable.

El derecho de información a los empleados se puede hacer efectivo mediante una cláusula/anexo incorporada/o al contrato laboral, por ejemplo; o mediante comunicados internos a la plantilla. Si para la implantación del registro de la jornada el empleador utiliza datos personales de los trabajadores obtenidos a través de sistemas de geolocalización, deberá informar expresamente a los trabajadores acerca de la existencia y características de estos dispositivos¹⁶.

Este derecho de información está muy vinculado con el de transparencia ¹⁷ por el que la empresa responsable debe realizar la información al trabajador de una forma concisa, transparente, inteligible y de fácil acceso, debiendo utilizarse un lenguaje claro y sencillo.

Con ocasión de la información que el empleador ha facilitado a los trabajadores, éstos conocerán los derechos que les asisten en los términos del art. 15 a 22 RGPD, y podrán ejercer el derecho de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad (según proceda). Para el ejercicio de estos derechos por los trabajadores, la empresa deberá habilitar los medios necesarios y establecer procedimientos internos para canalizar las solicitudes de esos derechos (por ejemplo mediante formularios disponibles para los trabajadores).

Solo la empresa podrá tratar los datos personales de sus trabajadores cuando el tratamiento este amparado en algunas de las causas de legitimación dispuestas en el art. 6 RGPD. ¿Debería la empresa solicitar el consentimiento de todos los trabajadores para el tratamiento de sus datos por la implantación del registro de la jornada? Según establece la AEPD, el tratamiento de datos personales de los trabajadores derivado de la implantación del registro de jornada es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento establecida en el artículo 6.1.c RGPD. Por ello, para la implementación del registro de jornada no se precisa el consentimiento del trabajador, siendo base suficiente de legitimación la propia norma laboral, cuyo artículo 34.9 ET establece la obligación de las empresas de realizar dicho registro de la jornada con carácter individual de cada persona trabajadora.



16 Art. 90 RGPD.
17 Art. 12 RGPD.

Ahora bien, si a través del sistema de registro se recogen, por ejemplo, datos del trabajador que tienen la consideración de “datos biométricos”, además de la base de legitimación necesaria del art. 6 RGPD, deberemos tener en cuenta la máxima protección que el RGPD otorga a estos “datos biométricos”, pues según hemos visto previamente tienen la consideración de “categoría especial de datos” (al igual que aquellos datos referentes a la ideología política, orientación sexual o datos de salud, por ejemplo).

A la vista de esta consideración como datos de especial protección ¿puede tratar el empresario responsable “datos biométricos” de los trabajadores en la implantación del registro? El artículo 9.1 del RGPD establece, como regla general, la prohibición del tratamiento de este tipo de datos, si bien esta prohibición no se aplica en los supuestos enumerados en el artículo 9.2 RGPD, entre los que se encuentra – en su apartado b - cuando “el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral”. Por ello, esta excepción de la norma permite la utilización de “datos biométricos” por el empleador para el control diario de la jornada y acreditación del cumplimiento del contrato laboral; en concreto por el cumplimiento de una obligación legal de garantizar el registro de la jornada laboral (los artículos 20 y 34 del Estatuto de los Trabajadores). En este mismo sentido, y en relación a la utilización de sistema de control con tecnologías biométricas de huella dactilar o de reconocimiento facial, la AEPD ha considerado¹⁸ que “el uso de estas tecnologías podría considerarse una medida de control por el empresario admitida por el artículo 20 ET, siempre y cuando sea proporcional, lo que exigiría tener en cuenta la naturaleza de la actividad y de las instalaciones para cuyo acceso se requiriese el reconocimiento...”.

De forma independiente al sistema o medio elegido para implantar el registro, el tratamiento de los datos personales de los trabajadores debe realizarse siempre respetando los principios recogidos en el art. 5 RGPD (licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad y principio de “responsabilidad proactiva”).

Uno de los principios citados es el “principio de minimización de datos”, que determina que no sería lícito que la empresa recogiera y almacenara más datos personales de los trabajadores de los que realmente fueran necesarios para los fines del control diario de la jornada, por lo que “no se debe aprovechar la introducción de un sistema de control para implantar un sistema general de vigilancia del trabajador”¹⁹.

Si bien con motivo de la entrada en vigor del RGPD se ha suprimido la obligación de notificar ficheros a la AEPD para su inscripción en el Registro General de Protección de

.....

18 10ª Sesión Anual Abierta de la AEPD. 4 de junio de 2018.

19 EFE Madrid, 13 mayo 2019.

Datos ²⁰, ahora existe la obligación de elaborar el denominado Registro de Actividades de Tratamiento (RAT), que deberá contener la información señalada en el artículo 30 RGPD. Por ello, la empresa estará obligada a registrar el tratamiento en el RAT derivado del control diario de la jornada²¹. Este RAT no sería obligatorio para aquellas empresas que tengan menos de 250 trabajadores, pues están exentas de realizarlo (salvo cuando el tratamiento pueda entrañar un riesgo para las libertades y derechos de los trabajadores y se trate de datos de categoría especial). Esta excepción es importante, pues la mayoría del tejido empresarial español está compuesto por PYMES de menos de 250 trabajadores (99,8% del total del tejido empresarial ²²).

Uno de los aspectos que debe contener el RAT es el referente a “los plazos previstos para la supresión de las diferentes categorías de datos” (Art. 30.1.f RGPD y 31 LOPDGDD). Esta previsión debe reflejarse en el RAT teniendo en cuenta la contenida en el nuevo artículo 34.9 ET “...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.”. La empresa debe tener en cuenta este aspecto, y establecer un protocolo que regule la supresión de los datos en la empresa, por ejemplo, para cuando los datos de los empleados no sean necesarios en relación con los fines para los que fueron recogidos. Si bien, para los derivados del control de la jornada, al menos durante 4 años estarán a disposición de los propios trabajadores, de los representantes legales, así como de la Inspección de Trabajo y Seguridad Social, debiendo procederse, en los términos del artículo 32 LOPDGDD, en relación al bloqueo/ destrucción de los mismos.

En el supuesto de que la empresa (como “responsable de tratamiento”) contrate a otra empresa externa la implantación del sistema de registro de jornada, esta última se convertirá en “encargado de tratamiento”²³. Conforme al ya citado principio de responsabilidad proactiva, la empresa responsable deberá ser diligente en la elección del encargado de tratamiento, pues debe contratar únicamente a aquellos que ofrezcan garantías suficientes con el cumplimiento de las medidas técnicas y organizativas apropiadas. Esta empresa proveedora podrá acceder a los datos personales de los trabajadores necesarios para implantar el registro, siempre que exista un contrato de encargo, en donde se determinarán las instrucciones dadas por la empresa e igualmente se incorporarán las estipulaciones del art. 28 RGPD, las cuales obligan al encargado de tratamiento a su cumplimiento.

.....

20 Regulada en la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 y la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

21 El nivel de desagregación de las actividades de tratamiento es una decisión del responsable de tratamiento. Esta actividad de tratamiento pudiera denominarse control diario de la jornada o bien estar agrupada con otras en torno a una misma finalidad.

22 Cifras PyME. Datos junio 2019 publicados por Ministerio de Industria, Comercio y Turismo (<http://www.ipyme.org>).

23 Art. 28 RGPD.

Es importante que la empresa identifique también, con carácter previo a la implantación del sistema de registro, si el sistema elegido podría entrañar un “alto riesgo” en el tratamiento de los datos de los empleados, para lo cual la empresa (previo análisis preliminar de dicho tratamiento²⁴) debe determinar si tiene o no que realizar - lo que la norma denomina - una “evaluación de impacto”(EIPD)²⁵.El responsable de tratamiento puede considerar que un tratamiento que cumpla dos de los nueve criterios indicados por el Comité Europeo de Protección de Datos ²⁶ (o de la lista no exhaustiva complementada por la AEPD²⁷) requerirá la realización de una EIPD.

En la práctica, esta evaluación supone una herramienta preventiva que permite determinar el nivel de riesgos de un determinado tratamiento, para así adoptar las medidas (controles) más adecuadas para minimizar el riesgo del tratamiento. Para su realización la EIPD debe contar con los siguientes elementos:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento.
- Evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad, y de los riesgos para los derechos y libertades de los interesados (juicio de ponderación).
- Medidas para mitigar esos riesgos.

En el supuesto que el resultado de la EIPD sea favorable, la actividad de tratamiento se realizará siempre que las medidas necesarias hayan sido implantadas. Si por el contrario, del resultado de la EIPD se determina que no es posible realizar el tratamiento, sería necesario utilizar el procedimiento de consulta previa a la Autoridad de Control²⁸.

¿Qué ocurre si el responsable de tratamiento no cumple con los requerimientos del RGPD en la implantación del registro diario de la jornada? Con carácter general, en función de la infracción y circunstancia de cada caso individual, el incumplimiento de la norma podría suponer la imposición de sanciones económicas por la autoridad de control (AEPD o autoridades autonómicas competentes) que pueden llegar a alcanzar los 10 millones de euros (o hasta el 2% del volumen de negocio total anual global del ejercicio financiero anterior) o, incluso hasta los 20 millones de euros (o hasta el 4% del volumen

.....

24 Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD. AEPD.

25 Art. 35.1 RGPD.

26 Grupo de Trabajo del Artículo 29 en la guía WP248 “Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679.

27 Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4).

28 Artículo 36 RGPD.

de negocio antes citado).²⁹ Estamos hablando de sanciones muy elevadas que pueden ser impuestas tanto a multinacionales como a pequeñas empresas, siendo claramente el impacto muy diferente en una y otra.

El nuevo modelo de supervisión del RGPD también establece medidas correctoras ante posibles incumplimientos de la norma que puede ser acordadas por la autoridad de control; tales como advertencias, apercibimientos, actuaciones específicas en un plazo determinado; o bien una limitación temporal o definitiva del tratamiento de los datos.

¿Y si el empleado considera que en la implantación del registro de la jornada se ha vulnerado la normativa en relación al tratamiento de sus datos personales y el ejercicio de sus derechos? El trabajador podrá presentar una reclamación ante la Autoridad de Control (AEPD o a las autoridades autonómicas competentes), y tendrá derecho a acudir a los tribunales de justicia, y a solicitar una indemnización por los daños y perjuicios materiales o inmateriales causados como consecuencia de la infracción.

Si se tratara de posibles infracciones de otros empleados, el trabajador puede igualmente poner en conocimiento de la empresa la existencia de esas conductas a través de una denuncia interna³⁰, debiendo la propia empresa poner a disposición de los trabajadores canales o circuitos para su tramitación junto con medidas que garanticen la confidencialidad³¹. Por tanto, los trabajadores pueden ser en cualquier caso, bien denunciantes o denunciados.

2.2. Implantación de dispositivos para el control diario de la jornada que tratan datos biométricos de los empleados

El art.10 del Real Decreto-ley 8/2019 no establece una modalidad específica o predeterminada para el registro diario de la jornada, limitándose a señalar que se debe llevar a cabo día a día, e incluir el momento de inicio y finalización de la jornada. En este marco, para cumplir la norma, la empresa puede utilizar cualquier sistema que proporcione información fiable y no sea manipulable, ya sea en soporte papel o telemático.

Las empresas deben decidir cuál es la mejor solución para el registro de la jornada. El sistema biométrico de control de presencia es un sistema muy utilizado, y especialmente el sistema de fichaje mediante huella dactilar, pues parece que “la biometría es la única llave que no se puede falsificar, copiar o perder”³².

.....

29 La LOPDGDD establece que constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.

30 Informe Jurídico de la AEPD núm. 0128/2007, sobre creación de sistemas de denuncias internas en la empresa.

31 Artículo 24 LOPDGDD.

32 <https://innovadores.larazon.es/10 Mayo 2019>.

Los sistemas biométricos de control de presencia pueden requerir la autenticación de la identidad del trabajador a través del iris del ojo, de la retina, palma de la mano³³ facciones, la voz, el modo de caminar, o bien a través de la huella digital (basada en el principio de que no existen dos huellas dactilares exactamente iguales).

Las herramientas biométricas pueden ser estáticas, que miden y tratan características como la huella dactilar o la forma de la cara; o dinámicas, nuevas herramientas tecnológicas que pueden recoger las características del comportamiento de las personas (análisis de información del uso del teclado, la forma o cadencia de caminar, conducta gestual, por lo que de esta forma se reconoce la identidad de una persona...).

A la vista de la tecnología disponible en estos sistemas, y de los datos de especial protección que se tratan (Art. 9 RGPD), las empresas previamente a su implantación deberán ponderar la necesaria proporcionalidad del sistema de control a elegir, analizar el riesgo y garantizar las medidas adecuadas. Se incorpora así otro concepto, el de la proporcionalidad en la utilización de sistemas para el control de la jornada laboral. No hay que dar por sentado que la implantación de cualquier sistema de control horario que recoja datos biométricos de los empleados es proporcional, y por tanto, conforme con el RGPD (principio de minimización).

Este asunto ha sido tratado en determinados dictámenes e informes de las autoridades de control estatales (Dictamen 16/045 de la Agencia Vasca de Protección de Datos, relativo a la implantación de la huella dactilar como medio de fichaje; Dictamen CNS 63/2018 de la Autoridad Catalana de Protección de Datos en relación con la consulta formulada por un colegio profesional sobre la utilización de sistemas de control basados en la huella dactilar; o Informe 0065/2015 del Gabinete Jurídico de la Agencia Española de Protección de datos (evacuado con anterioridad a la aplicación del RGPD) en relación al sistema de control biométrico de los alumnos del Centro para su acceso al comedor), en los cuales se determina que, al tratarse de datos de especial protección, es recomendable evaluar la necesidad de implantar otro tipo de sistemas que, sin utilizar esta categoría de datos especialmente protegidos, permitan alcanzar el mismo fin. Este sistema de registro con datos biométricos solo debería ser de aplicación si no hay otros medios que sean menos intrusivos que se puedan implantar, debiéndose acompañar para ello de garantías adecuadas.

Tal y como ha señalado la AEPD³⁴ en diferentes informes, en caso de ser posible deberían instalarse preferentemente “sistemas de reconocimiento de huella dactilar” sin que el sistema tuviera que almacenar el dato biométrico (*por ejemplo, una tarjeta inteligente que se contrastase con la huella y se mantuviera siempre en poder del trabajador*). Por lo tanto, la empresa no tendría almacenado el dato biométrico.

.....

33 STSJ de Cantabria, de 10 de enero de 2003.

34 Sesión anual abierta de la AEPD de 04 de junio de 2018.

Al respecto, el Comité de Ministros del Consejo de Europa adoptó el 1 de abril de 2015 la Recomendación CM/Rec (2015) 5 relativa al tratamiento de datos personales en el entorno laboral. En su principio general nº 18, se establece que la recogida y tratamiento de los datos biométricos no debería realizarse, salvo en los casos en que sea necesario para la protección de los intereses legítimos de los trabajadores, de los empresarios o de terceros, y ello solo como última opción, cuando sea imposible utilizar otros métodos alternativos de tratamiento menos intrusivos y siempre que su tratamiento se acompañe de las garantías apropiada. De igual forma entiende que el tratamiento de datos biométricos debe basarse en métodos científicamente reconocidos y sometidos a las exigencias estrictas de seguridad y proporcionalidad.

Este sistema biométrico de control de presencia es uno de los posibles que el empleador puede implantar. También puede decantarse por otros, en los que el sistema de registro elegido pueda requerir el acceso a dispositivos digitales o bien del uso de sistemas de video vigilancia o de geolocalización³⁵. Cualquier sistema que el empleador utilice, deberá previamente ponderar la proporcionalidad del sistema de control, analizando el riesgo o, en su caso, evaluando el impacto (EIPD), y adoptando las medidas de seguridad adecuadas.

Estos sistemas irán evolucionando tecnológicamente y, con ellos, la necesidad de una mayor regulación para la protección de los datos personales. Por ejemplo, una empresa belga ha implantado a varios de sus empleados, de manera voluntaria, un “chip” bajo la piel que funciona como una llave de identificación para abrir puertas o acceder al ordenador³⁶. En un futuro cercano, es posible que asistamos con normalidad al uso de sistemas de implantación de chips subcutáneos en trabajadores que permitan su geolocalización, o para controlar determinados dispositivos (tecnología domótica), o incluso ser utilizado para el sistema de fichaje de entrada y salida por los empleados en la empresa.

3. LOS DENOMINADOS “DERECHOS DIGITALES” EN LA NUEVA LOPDGDD: LA DESCONEXIÓN DIGITAL Y OTROS DERECHOS DE APLICACIÓN EN EL ÁMBITO LABORAL

Tal y como dispone el Apartado IV del Preámbulo de la LOPDGDD, una deseable futura reforma de la Constitución debiera incluir, entre sus prioridades, la actualización

.....

35 SAN nº. 13/2019 de 6 febrero (Sala de lo Social, Sección 1ª): al ser los datos de localización de una persona un dato de carácter personal, cualquier actuación empresarial que incida sobre los mismos afecta al derecho la privacidad del trabajador protegido por los arts 18.1 y 4 de la CE (STC 186/2000).

36 ABC Economía 03/02/2017. La sociedad belga de marketing digital “Newfusion” implanta un «chip» de identificación bajo la piel de sus empleados.

de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, mientras tanto no se acometa este reto, el legislador ha abordado el reconocimiento de un sistema de garantía de los derechos digitales con la promulgación de la citada LOPDGDD. Esta “Ley Orgánica” incorpora, en su título X, la denominada “*garantía de los derechos digitales*” (que el RGPD no reconoce), y en su *disposición final 13 y 14* añade un nuevo *artículo 20 bis* al Estatuto de los Trabajadores (ET), y una nueva *letra j bis* al artículo 14 del Estatuto Básico del Empleado Público (EBEP).

La LOPDGDD acomete la tarea de reconocer y garantizar un elenco de *derechos digitales* de los ciudadanos conforme al mandato establecido en la Constitución (artículo 18.4), derechos que suponen una prolongación de los derechos de las personas llevados al mundo digital. En la norma se incorporan una serie de derechos fundamentales de los trabajadores en el ámbito de la sociedad digital, viniendo a destacar, en este artículo, el denominado “*derecho a la desconexión digital en el ámbito laboral*”, que se regula junto con otros derechos en los que se garantiza la intimidad del trabajador (ante el uso de dispositivos digitales, dispositivos de video vigilancia y de grabación de sonidos en el lugar de trabajo, y ante la utilización de sistemas de geolocalización en el ámbito laboral).

En todos ellos destaca, como elemento común, la necesaria información y transparencia hacia el trabajador/empleado público, garantía de la buena fe que debe presidir la relación contractual, y la necesaria aplicación (prevista en art. 89.3 LOPDGDD) del principio de proporcionalidad, el de intervención mínima y el resto de garantías previstas en su articulado.

¿Cómo debe respetar el sistema de registro diario de la jornada del artículo 34 ET el ejercicio de los derechos digitales de los empleados? En el supuesto de que la aplicación/software utilizada/o por el empleador en el registro de la jornada incorpore tecnologías tales como video vigilancia o sistema de geolocalización, deberá ser comunicada a los empleados y a la representación de los trabajadores, debiendo ser respetuoso igualmente con el derecho de los trabajadores a que no sea vulnerada su intimidad. Puede darse el caso de geo localizadores situados en los dispositivos móviles, automóviles... que permiten el control empresarial del trabajador, si bien solo se podrán utilizar durante la jornada laboral, tal y como se pronuncia la STSJ de Asturias de 27 de diciembre de 2017³⁷. Esta Sentencia considera que la instalación de los dispositivos GPS en los vehículos como medida de vigilancia es ajustada a derecho, no existiendo lesión del derecho a la intimidad por parte del empresario; si bien se estima la vulneración de dicho derecho fundamental por estar activado el GPS también a partir de la finalización de la jornada laboral, sin el imprescindible consentimiento de los trabajadores en este supuesto. El tribunal considera que una vez finalizada la jornada laboral se debe desactivar el localizador GPS.

.....

37 STSJ Asturias, de 27 de diciembre de 2017, núm. 3058/2017 (AS 2018, 296).

Este pronunciamiento tiene relación con uno de los derechos digitales recogidos en el artículo 20 bis del Estatuto de los Trabajadores, y letra j bis) del artículo 14 del Estatuto Básico del Empleado Público, el denominado “derecho a la desconexión digital”, que se remite a lo dispuesto en el artículo 88 de la LOPDGDD, y por el que se garantiza a los trabajadores y empleados públicos que se respete su tiempo de descanso, de permisos y vacaciones, así como su intimidad personal y familiar, fuera del tiempo de trabajo legal o convencionalmente establecido³⁸. Se establece que las modalidades del 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.

En Alemania, empresas como Volkswagen o Daimler-Benz y BMW han sido pioneras en la firma de acuerdos en relación a la “desconexión tecnológica”, con el objetivo de “limitar o impedir el riesgo derivado del uso excesivo de las nuevas tecnologías” y combatir “la ilusión de un recurso humano disponible las veinticuatro horas del día, todos los días al año”.

El debate sobre el citado derecho ha llegado a España hace unos años, precisamente a raíz de la regulación del derecho a la desconexión (*droit à la déconnexion*) que ha sido regulado en Francia como medida incluida en la reforma de su ley laboral, en vigor desde el 01 de enero del 2017 (Loi 2016-1088, de 8 de agosto de 2016, conocida como Loi Travail), incorporando por primera vez el ejercicio de este derecho³⁹.

En nuestro país han existido algunos pronunciamientos de los Tribunales de Justicia de interés a este respecto y algunas regulaciones internas de empresas (previas a la entrada en vigor de la LOPDGDD) que han venido incorporando el citado derecho:

- SAN de 17.7.1997 (120/1997), que declaró la nulidad de las instrucciones de la empresa que obligaban a los empleados a “mantener la atención a sus teléfonos móviles una vez finalizada la jornada de trabajo de cada uno de ellos”.
- STSJ Castilla y León de 3.2.2016, que determina que las empresas que utilizan TIC o teletrabajo, en el domicilio o a distancia, deben disponer de políticas de gestión del tiempo, tal como procedimientos de conexión, medios de control y registros de jornada, para afrontar posibles reclamaciones sobre excesos de jornada, seguridad y salud laboral (por exceso de conexión y estrés laboral, sobre todo).

.....

38 “*The right to privacy*” (*El derecho a la intimidad*), ensayo publicado por los juristas norteamericanos Samuel Warren y Louis Brandeis en 1890, se considera la génesis de la protección de la privacidad, refiriéndose al “derecho a estar solo” como el derecho a no ser molestado (*the right to be let alone*).

39 <http://noticias.juridicas.com/actualidad/noticias>.

- Juzgado de lo Social nº14 de Madrid (auto de 4 Jul. 2019, Rec. 56/2019). Se plantea cuestión de inconstitucionalidad sobre el art. 162.2 LEC que da por notificada una resolución remitida vía “Lexnet” a los 3 días con independencia de que se haya accedido a su contenido o no, considerando el juzgador que “Lexnet” pudiera no garantizar el derecho de desconexión de abogados y procuradores.
- Convenio Colectivo del Grupo AXA ⁴⁰, que establece en su art. 14 el derecho a la desconexión digital, al entenderse que la conectividad permanente está afectando al ámbito personal y familiar de los trabajadores/as, por lo que las partes firmantes “coinciden en la necesidad de impulsar el derecho a la desconexión digital una vez finalizada la jornada laboral”.
- XVI Convenio Colectivo de la ONCE y su personal ⁴¹, en cuyo apartado “áreas de intervención para la consecución de los objetivos del plan de igualdad” establece, como medida que promueve la conciliación de la vida personal, laboral y familiar, la denominada desconexión digital “aplicada a herramientas de índole tecnológica e informática, como teléfonos y tablets con conexión de datos y ordenadores portátiles, compartiendo que su utilización no ha de ser motivo ni argumento para la extensión de la jornada laboral, ni para la interrupción de los tiempos de descanso o licencias de los trabajadores y trabajadoras”.
- El acuerdo horario de IKEA, en vigor desde el 01 septiembre de 2018, establece en su artículo 13 la desconexión digital, por el que los trabajadores “tienen derecho a no responder a cualquier tipo de comunicación por cualquier canal (correo electrónico, teléfono, WhatsApp, redes sociales...etc), fuera de su horario de trabajo, salvo causa de fuerza mayor”.

Las empresas abogan cada vez más por permitir a los trabajadores y equipos de trabajo, precisamente, al amparo de los dispositivos tecnológicos (especialmente los de conexión remota), una gran autonomía en la gestión de su tiempo de trabajo, y una flexibilización mayor sobre el lugar de prestación de servicios. En este ámbito los avances tecnológicos imponen un nuevo modelo de bienestar, donde no existe separación entre el trabajo y la vida privada, suponiendo una mayor implicación del trabajador con la empresa y su realización a través del trabajo (“*blending*”). Esto contrasta con la necesidad de la empresa de proteger la salud del empleado, de evitar que el tiempo de trabajo invada el tiempo de descanso de los trabajadores, y su esfera familiar y personal, pues la facilidad de conexión



40 Resolución de 21 de septiembre de 2017, de la Dirección General de Empleo, por la que se registra y publica el Convenio colectivo del Grupo Axa. (BOE 10/10/2017).

41 Resolución de 8 de enero de 2018, de la Dirección General de Empleo, por la que se registra y publica el XVI Convenio colectivo de la ONCE y su personal (BOE 18/01/2018).

con el trabajo a través de medios tecnológicos posibilita que se diluya la separación entre tiempo de trabajo y descanso. Sobre este aspecto deben trabajar las empresas en el marco del derecho a la desconexión, evitando la presión que los dispositivos digitales proporcionados por el empresario imponen sobre los trabajadores, evitando los efectos perjudiciales sobre su salud (estrés, cansancio, agotamiento mental y cognitivo...).

Es importante que este derecho a la desconexión digital del trabajador sea compatible con las medidas organizativas de la propia empresa, como es la obligación de garantizar el registro diario de la jornada del art. 34 ET.

La norma establece expresamente que se deberá preservar 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. Es en relación a las distintas formas de realizar este trabajo donde puede existir un especial conflicto, pues debe ser compatible la obligación de fichar del empleado junto con el derecho del mismo a la desconexión digital. Para ello es conveniente protocolizar en la empresa las modalidades del ejercicio de la desconexión según se trate de trabajadores de presencia en el centro de trabajo, a distancia (total o parcial), trabajadores en domicilio; y también trabajadores que tengan horario regular, horario flexible o con autogestión de su tiempo de trabajo⁴². Esta situación puede ser resuelta por la empresa estableciendo fórmulas adecuadas que permitan fichar a estos trabajadores; por ejemplo, a través de la actividad monitorizada de los dispositivos electrónicos que se hallen a disposición del trabajador.

Una vez clarificadas estas situaciones, identificando para ello a partir de qué horario se deben respetar los tiempos de descanso para el trabajador, podemos entender que el registro diario de la jornada posibilitará el derecho a la desconexión digital, pues será una forma de conocer el momento en el cual el empleado está trabajando o bien deja de hacerlo, teniendo derecho a no ser molestado fuera de su jornada laboral. Por ello, un adecuado registro de la jornada de trabajo puede contribuir a la consecución del objetivo del derecho a la desconexión, puesto que a través del mismo puede comprobarse el cumplimiento de la jornada laboral, la realización de exceso de jornada ordinaria, y determinar si se está respetando o no el derecho al descanso de los trabajadores.

Es evidente que las nuevas tecnologías, y las nuevas formas de entender el trabajo (y el concepto de trabajador) está generando una nueva casuística en la aplicación de la norma, que nos abre a nuevos escenarios que deberán interpretarse, o bien regularse.

.....

42 A este respecto la “Guía sobre el Registro de Jornada del Ministerio de Trabajo, Migraciones y Seguridad Social”, establece que “en relación con los modos de organización del trabajo que se basan en fórmulas de flexibilidad del tiempo de trabajo y de distribución irregular de la jornada, incluido el trabajo a distancia o teletrabajo y horarios flexibles del trabajador, dentro siempre de los límites legales y convencionales aplicables, el registro diario de jornada ni obsta su operatividad ni constituye impedimento alguno a su continuidad o ampliación, considerándose un elemento que garantiza la acomodación a las necesidades empresariales y a los intereses de conciliación de los trabajadores, familiares o de otro tipo.

Todas estas cuestiones que se plantean es recomendable que sean incorporadas en la política interna establecida por el empleador (art. 88.3 LOPDGDD), y dirigida a los trabajadores (un protocolo de desconexión digital), previa audiencia a los representantes de los trabajadores. Este protocolo debiera definir especialmente las modalidades del ejercicio del derecho a la desconexión, las acciones de formación y las acciones de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas.

Un ejemplo muy significativo y actual de cuál pueda ser la política interna de una empresa, en el marco de la regulación del derecho a la desconexión digital de los trabajadores según acuerdo con los sindicatos, es la realizada por la entidad Telefónica.

El 23 de noviembre de 2018, previa a la entrada en vigor de la LOPDGDD, Telefónica firma con los sindicatos un acuerdo de sensibilización en materia de desconexión digital, por el que “se compromete a impulsar medidas para potenciar el respeto al tiempo de descanso de los trabajadores una vez finalizada la jornada laboral, reconociendo el derecho a la desconexión digital como elemento fundamental para lograr una mejor ordenación del tiempo de trabajo en aras del respeto de la vida privada y familiar y, en definitiva, de la calidad de vida y salud de los trabajadores”. Posteriormente, en fecha de 17 de Julio de 2019, la entidad Telefónica firma junto con los sindicatos UGT y CCOO una “política interna reguladora del derecho a la desconexión digital de las personas trabajadoras de telefónica”, destacando en ella cuestiones como:

- Reconoce el derecho a la desconexión digital como un derecho, no como una obligación. Esto supone que las personas trabajadoras que realicen comunicaciones fuera del horario podrán hacerlo con total libertad; sin embargo, deben asumir que no tendrán respuesta alguna hasta el día hábil posterior. En caso de enviar una comunicación que pueda suponer respuesta fuera del horario establecido al efecto, el remitente asumirá expresamente que la respuesta podrá esperar a la jornada laboral siguiente. De interés es el debate acerca de si estamos ante un derecho, o también ante una obligación del trabajador. Si bien pudieran plantearse infracciones disciplinarias derivadas del incumplimiento del citado derecho por parte de los empleados, parece razonable considerar que la desconexión digital supone un derecho (no una obligación) y no resultaría procedente penalizar al trabajador por ello, si bien no resultará fácil el cumplimiento del mismo si no se cuenta con su colaboración.
- Las personas trabajadoras tendrán derecho a no responder a ninguna comunicación, fuere cual fuere el medio utilizado (correo electrónico, Whatsapp, teléfono, etc...) una vez finalizada su jornada laboral, salvo que concurren circunstancias de causa de fuerza mayor o que supongan un grave, inminente o evidente perjuicio empresarial o del negocio. En este último caso, el tiempo de trabajo así requerido

podría calificarse como hora extraordinaria. En la política interna de las empresas, en especial en determinados sectores, debieran identificarse situaciones extraordinarias o de fuerza mayor en las que se pudiera contactar con el empleado fuera de la jornada ordinaria. Otra cuestión diferente es la consideración como hora extraordinaria, cuestión que genera una casuística importante.

- Quienes tengan la responsabilidad sobre un equipo de personas deben cumplir especialmente las políticas de desconexión digital.

La LOPDGDD no establece ningún régimen sancionador a la empresa por no cumplir con la obligación de establecer una política interna en esta materia, si bien podría considerarse que es una vulneración de los derechos de jornada y podría dar lugar a una infracción grave de la LISOS, pudiendo agravarse la sanción si se entiende que entramos en el terreno de los riesgos psicosociales de los trabajadores.⁴³

La LOPDGDD incorpora en su articulado otra serie de derechos aplicables en el ámbito de las relaciones laborales, que tienen una base tecnológica o digital:

- Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral⁴⁴. La norma hace referencia a la protección a la intimidad de trabajadores y empleados públicos en el uso de los dispositivos digitales que la empresa ha puestos a su disposición (ordenadores portátiles, smartphone...). La empresa únicamente puede acceder a los contenidos de los mismos a efectos de controlar el cumplimiento de las obligaciones laborales y de garantizar la integridad de dichos dispositivos. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales y regular, no solo el uso adecuado por parte de los trabajadores del mencionado dispositivo digital como instrumento de trabajo, sino también el alcance del control empresarial de ese uso y la manera de llevarse a cabo el mismo cuando se haya admitido su uso con fines privados, debiendo participar los representantes de los trabajadores. La política de la empresa debe ser nítida y transparente, especificando de modo preciso los usos autorizados y en qué períodos pueden ser ejercidos. Los trabajadores serán informados de los criterios de utilización de los dispositivos, evitando así situaciones conflictivas con el empleador y vulneradoras de derechos⁴⁵.

43 <https://cincodias.elpais.com/>: “¿Cuándo se vulnera el derecho a la desconexión digital del empleado y cómo se sanciona?”

44 Artículo 87 LOPDGDD.

45 La Sentencia del Tribunal Europeo de Derechos Humanos (TEDH) 5.9.2017 (asunto Barbulescu-II), que revoca el criterio de la STEDH 12.1.2016 (Barbulescu-I), indica que “es una vulneración del derecho a la intimidad y al secreto de las comunicaciones vigilar los mensajes enviados por un trabajador mediante medios propios de la empresa y acceder al contenido de los mismos, si no ha sido previamente informado de esta posibilidad, incluso si existían normas en la empresa que prohíban su utilización con fines personales”.

- Derecho a la intimidad frente al uso de dispositivos de video vigilancia y de grabación de sonidos en el lugar de trabajo⁴⁶. Según este artículo los empleadores pueden tratar las imágenes recogidas por los sistemas de video vigilancia para el control de los trabajadores prevista en el artículo 20.3 del Estatuto de los Trabajadores, o de los empleados públicos prevista 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 a los trabajadores o empleados públicos, con carácter previo y de forma expresa, clara y concisa, acerca de esta medida. Es de interés la Sentencia del Tribunal Europeo de Derechos Humanos (TEDH) de 9 de enero de 2018, en relación a la vigilancia oculta, que establece que ha de tenderse hacia un uso excepcional y muy limitado de la misma, por lo que debe procurarse, en la medida de lo posible, el empleo de medidas menos invasivas. Si la video vigilancia resultara imprescindible, su uso deberá limitarse al máximo en cuanto a destinatarios, espacios y tiempos. Solo si la medida obedece a una proporcionalidad muy rigurosa y ajustada tendrá posibilidades de que sea admitida como una prueba no atentatoria contra derechos fundamentales.
- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.⁴⁷ Los empleadores pueden tratar los datos obtenidos de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o 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. A este respecto es de interés la reciente *Sentencia de la Audiencia Nacional nº. 13/2019 de 6 febrero* (Sala de lo Social, Sección 1ª) en referencia al denominado “Proyecto Tracker” de la empresa Telepizza. La citada Sentencia determina la nulidad de la implantación de un sistema de geolocalización por parte de la empresa Telepizza, por la que el trabajador debería aportar un teléfono móvil con conexión a internet de su propiedad, y descargarse una App (realizada por la empresa) para implantar un sistema de geolocalización, a través de la cual la empresa conocería la situación de su dispositivo, y por ello del trabajador durante su jornada laboral. La Sentencia determina que el “Proyecto Tracker” vulnera el derecho a la privacidad de los trabajadores pues:
 - a) La medida implantada no supera el necesario juicio de proporcionalidad. La misma finalidad se podría haber obtenido con medidas que suponen una menor injerencia en los derechos fundamentales de los empleados como pudiera ser

46 Artículo 89 LOPDGDD.

47 Artículo 90 LOPDGDD.

la implantación de sistemas de geolocalización en las motocicletas en las que se transportan los pedidos o las pulseras con tales dispositivos que no implican para el empleado la necesidad de aportar medios propios, ni datos de carácter personal - como son el número de teléfono o la dirección de correo electrónico - en los que han de recibir el código de descarga de la aplicación informática que activa el sistema.⁴⁸

b) Para la implantación del sistema de geolocalización por parte del empleador se ha prescindido de informar a los trabajadores en los términos a que se refieren los arts. 12 y 13 del RGPD, (y art.11 y 90 de la LOPDGDD). La información que se le dio a la RLT⁴⁹ igualmente resultó insuficiente. La Sentencia hace referencia al art. 90.2 LOPDGDD (si bien no se encontraba en vigor ese texto legal), que establece la necesaria información que debe proporcionarse a los trabajadores y a sus representantes con carácter a previo a la instalación de sistemas de geolocalización.

4. CONCLUSIONES

Según hemos visto, las empresas deben implantar obligatoriamente un registro diario de la jornada según dispone el *artículo 34.9* del ET, y deben hacerlo cumpliendo con lo dispuesto en el RGPD utilizando mecanismos que no sean “desproporcionados”. Desde la publicación del Real Decreto Ley 8/2019, de 8 de marzo, las empresas han tenido dos meses de “vacatio legis”⁵⁰ para implantar el registro, siendo un breve plazo de tiempo durante el cual han debido considerar todos los aspectos necesarios para crear un marco de seguridad jurídica en las relaciones laborales (interlocución con los sindicatos; información a los trabajadores, diseño y gestión del registro, software adecuado para cumplir con el objetivo de la norma...), junto con otros aspectos que son igualmente de obligado cumplimiento: los relativos a la protección de los datos personales que se traten de los empleados. Dentro del marco de la responsabilidad proactiva, la denominada protección de datos desde el diseño y por defecto⁵¹ obliga a la empresa a que, cuando un producto o servicio que implique el tratamiento de datos comienza a diseñarse, deben tenerse en

.....

48 “Estas limitaciones o modulaciones tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes” (STC 98/2000).

49 Representación Legal de los Trabajadores (RLT).

50 Disposición final sexta, apartado 4º, del Real Decreto-ley 8/2019, de 8 de marzo.

51 Artículo 25 RGPD.

cuenta desde el principio también todas las cuestiones relativas a la protección de datos personales y solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Con carácter previo a la implantación del registro, la empresa deberá ponderar la necesaria proporcionalidad del sistema elegido y el cumplimiento de las garantías adecuadas en el tratamiento de los datos personales de los empleados. El empleador puede elegir entre diferentes métodos para cumplir con el control horario de sus trabajadores, existiendo herramientas tecnológicamente muy avanzadas que suponen un alto riesgo de vulneración de los derechos fundamentales de los trabajadores, por el carácter agresivo de estos mecanismos y por los derechos que pueden resultar afectados (sistemas de geolocalización, video vigilancia, sistemas biométricos (estáticos o dinámicos)....).

Las organizaciones y empresas deben apostar por implantar políticas de protección de datos y de seguridad que supongan un compromiso claro de la dirección en esta materia, junto con el necesario asesoramiento de personal cualificado en protección de datos debido a la complejidad de la norma. Estas actuaciones ayudarán a prevenir y a adelantarse a los problemas legales que puedan surgir en este ámbito, evitando las consecuencias que una mala gestión pueda ocasionar a los titulares de los datos y a la propia organización, ya sean daños tangibles (como los económicos) como intangibles (especialmente los que suponen pérdida de reputación).

En segundo lugar, es destacable el margen de actuación que el RGPD ha otorgado a los convenios colectivos o de empresa en la regulación específica del tratamiento de datos en el ámbito laboral. La norma le otorga flexibilidad en su regulación siempre dentro del marco de cumplimiento de la misma, teniendo gran relevancia la elaboración de protocolos internos y acuerdos derivados de la negociación colectiva que eviten cierta inseguridad jurídica en la empresa, 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, 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 de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral⁵². Existe igualmente un margen amplio de regulación interna en convenios colectivos que pueden establecer garantías adicionales en relación a los derechos digitales en el ámbito laboral.⁵³

En tercer lugar, en relación al derecho a la desconexión digital (como especificación “tecnológica” del derecho al descanso laboral), se trata de un derecho cuya realización está



52 Considerando 155 RGPD.

53 Derechos digitales en la negociación colectiva (Artículo 91 LOPDGDD).

igualmente condicionada a su desarrollo en convenio colectivo, o bien a un acuerdo empresa, pacto extra estatutario o cualquier otra manifestación de la autonomía colectiva. Sin perjuicio de ello, se deja en manos del empresario la puesta en marcha de la *política interna* dirigida a los trabajadores; eso sí, de conformidad con lo establecido en el convenio colectivo o acuerdo de empresa y previa audiencia a los representantes de los trabajadores. Parece ser que las empresas no están aún lo suficientemente concienciadas de la necesidad de hacer efectivo este nuevo derecho, que recordemos su reconocimiento se ha realizado por Ley Orgánica. Hubiera sido deseable que la norma estableciera un plazo razonable de tiempo que obligase a las empresas a la puesta en marcha de manuales o protocolos para el ejercicio del citado derecho, pues este derecho conecta directamente con la normativa reguladora del descanso (arts. 34 a 38 ET) y la salud laboral de los trabajadores (art.14,15 y 22 LPRL⁵⁴), por lo que su incumplimiento podría conllevar sanciones con encaje en la LISOS⁵⁵.

Aunque la nueva LOPDGDD en su Título X (“derechos digitales”) incorpora una “mezcla” de cuestiones relativas a la intimidad de los trabajadores en el entorno digital junto con otras relativas al *derecho de acceso universal a Internet, a la seguridad digital, a la educación digital o al derecho al testamento digital* (entre otros), su regulación ha sido una buena noticia al incorporar aspectos relativos al ámbito laboral que, de alguna forma, se venía demandando por parte de la doctrina y que la jurisprudencia ha ido guiando. Es cierto que no se van a cerrar todas las controversias que puedan presentarse en este ámbito, si bien proporcionará una mayor seguridad jurídica en las relaciones laborales.

BIBLIOGRAFÍA

CAMPO ESTAÚN, S. DEL, “Registro de jornada o crónica de un caos anunciado”, *El siglo de Europa*, nº 1294 (17 mayo), 2019.

CUADROS GARRIDO, M.E., “El uso del WhatsApp en las relaciones laborales”. *Nueva Revista Española de Derecho del Trabajo*, núm. 171, 2014.

GARCÍA-PERROTE ESCARTÍN, I., MERCADER UGUINA, J.R., “El control biométrico de los trabajadores”. *Revista de Información Laboral*, núm. 3, 2017.

GARCÍA SALAS, A.I., “El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2018”. *Revista de Información Laboral* núm. 2, 2018.

54 Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

55 Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.

JURADO CABALLERO, M. T., “El registro de la jornada de trabajo”, *Frisona española*, Año 39, nº 230, 2019.

LAHERA FORTEZA, J., “Respuestas a problemas prácticos del deber de registro diario de jornada”, *Observatorio de recursos humanos y relaciones laborales*, nº 146, 2019.

LÓPEZ-CANOSA FERNÁNDEZ, C., “A vueltas con el registro de jornada”, *Observatorio de recursos humanos y relaciones laborales*, nº 143, 2019.

LOUSADA AROCHENA, J.F., “Registro y control de la jornada de trabajo”, *Aranzadi Instituciones*, BIB 2016/85595.

MIRÓ MORROS, D., “El control de la jornada y el teletrabajo”. *Actualidad Jurídica Aranzadi* núm. 920, 2016.

ORTEGA GIMÉNEZ, A., “Cuestiones prácticas laborales en materia de protección de datos de carácter personal tras el nuevo reglamento general de protección de la datos de la UE”. *Revista Española de Derecho del Trabajo*, núm. 216, 2019.

- (2018), “El Reglamento General de Protección de Datos de la UE en la empresa: novedades prácticas” *Diario La Ley*, Nº 15, sección *Ciberderecho*.

PURCALLA BONILLA, M.A., “Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: Notas a propósito de la Ley 3/2018, de 5 de diciembre”. *Revista Española de Derecho del Trabajo*, núm. 218, 2019.

QUÍLEZ MORENO, J.M., “La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores”. *Revista Española de Derecho del Trabajo* núm. 217, 2019.

SEMPERE NAVARRO, A. V., “El registro empresarial de la jornada efectiva”, *Revista Aranzadi Doctrinal*, nº 6, 2017.

SERRANO ARGÜESO, M., “Always on. Propuestas para la efectividad del derecho a la desconexión digital en el marco de la economía 4.0”. *Revista Internacional y Comparada de relaciones laborales y derecho del empleo*. ADAPT University Press. Volumen 7, núm. 2, abril-junio 2019.

USHAKOVA, T., “De la conciliación a la desconexión tecnológica. Apuntes para el debate”. *Revista Española de Derecho del Trabajo*, 192, 2016.

VIDAL LÓPEZ, P., “El (no) registro de la jornada diaria de la plantilla”, *Actualidad jurídica Aranzadi*, nº 929, 2017.

JOSÉ ANTONIO MARCOS HERRERO

Abogado. Ilustre Colegio de Abogados de Málaga