• Junio 2019 • Secretaría Confederal de Acción Sindical y Gabinete Jurídico Confederal •

Informe

EL REGISTRO DE LA JORNADA DE TRABAJO

Especial consideración de los sistemas de registro y su impacto en materia de protección de datos

CCOO

EDITA: Confederación Sindical de CCOO

ELABORACIÓN: Secretaría Confederal de Acción Sindical y Gabinete Jurídico Confederal

Madrid, Junio de 2019

Índice

EL REGISTRO DE LA JORNADA DE TRABAJO

ESPECIAL CONSIDERACIÓN DE LOS SISTEMAS DE REGISTRO Y SU IMPACTO EN MATERIA DE PROTECCIÓN DE DATOS

Una vez realizada, por parte del Gabinete Jurídico Confederal, una primera aproximación a la aplicación práctica de la obligación de implantar en las empresas **un sistema de registro diario de la jornada** de cada persona trabajadora, y analizada la Guía sobre el registro de jornada, publicada por el Ministerio de Trabajo, Migraciones y Seguridad Social, el día 13 de mayo de 2019, resulta conveniente elaborar un nuevo documento en el que se analice con mayor profundidad, los sistemas o medios que pueden ser utilizados para el cumplimiento de esta obligación, y la necesidad, en mayor o menor medida, según el sistema que se implante, de respetar la normativa en materia de protección de datos y garantía de los derechos digitales, en relación con la esfera de privacidad, intimidad y dignidad de las personas trabajadoras.

Conviene antes de hacer el análisis más detallado de cada uno de los sistemas de registro, una serie de consideraciones previas, que deben tenerse en cuenta:

a) En primer lugar, es exigible, en todo caso, que exista una negociación colectiva con los RLT respecto a la organización y documentación del sistema de registro a implantar.

b) En segundo lugar, la norma nada dice respecto al sistema de registro que deba o pueda utilizarse, limitándose a señalar que cualquier sistema deberá, como mínimo, incluir el momento de inicio y finalización de la jornada diaria realizada; dicho esto, el resto, se remite a la autorregulación, mediante negociación colectiva o acuerdo de empresa.

c) En tercer término, el sistema elegido debe proporcionar información fiable, inmodificable y no manipulable ni alterable a posteriori. Apunta la Guía del Ministerio que *la información de la jornada debe documentarse 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.*

d) Y finalmente, se exige que los registros permanezcan a disposición de las personas trabajadoras, de sus RLT y de la Inspección de Trabajo, por lo que deben permanecer físicamente en el centro de trabajo o ser accesibles desde el mismo de forma inmediata y por tanto, no pueden estar o almacenarse en

otras oficinas de la empresa, en gestorías o terceros que gestionen los sistemas.

Veamos pues, que sistemas de registro más comunes se vienen utilizando y cuáles de ellos recogen y tratan datos de carácter personal de las personas trabajadoras, a fin de poder articular en la negociación colectiva los sistemas que sean menos invasivos en los derechos constitucionalmente protegidos, de intimidad y dignidad de los trabajadores y trabajadoras , y de negociarse la implantación de los mismos, que se garanticen los derechos de protección de datos, establecidos en el Reglamento Europeo de Protección de Datos 2016/67, de 27 de abril de 2016, relativo a la protección de las personas físicas (en adelante RGPD) y en la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales (LOPDPDG).

Los sistemas de registro, implantados ya en muchas empresas, o que pueden implantarse a partir de la entrada en vigor de la norma, se pueden agrupar en los siguientes tipos:

- SISTEMAS DE REGISTRO **EN PAPEL**
- SISTEMAS DE REGISTRO **CON FICHAJE POR TARJETA O NÚMERO (PIN)**
- SISTEMAS DE REGISTRO **BIOMÉTRICOS** (HUELLA DIGITAL O RECONOCIMIENTO FACIAL)
- SISTEMAS DE REGISTRO MEDIANTE **DISPOSITIVOS DIGITALES** (MOVIL, TABLET o PC)
- SISTEMAS DE REGISTRO POR **GEOLOCALIZACIÓN**

1. SISTEMAS DE REGISTRO QUE MENOR INCIDENCIA PRESENTAN EN MATERIA DE PROTECCIÓN DE DATOS

Entre estos sistemas, actualmente vienen utilizándose los de soporte papel o los fichajes por tornos o máquinas con tarjeta o números pin para cada trabajador/a.

1.1. SISTEMAS DE REGISTRO EN SOPORTE PAPEL

Este sistema posiblemente será el más usado en empresas pequeñas con escaso personal, ya que de un lado, no requiere asumir ningún tipo de coste, y de otro, su implementación es muy sencilla, basta la creación de una plantilla en la que conste, como mínimo, la hora de entrada y de salida diaria y la firma del trabajador.

No obstante, señalar que aunque **este sistema, desde el punto de vista de la protección de datos no entraña prácticamente ningún problema**, **es un sistema de**

registro no aconsejable puesto que resulta relativamente fácil su manipulación y alteración, entre otras cuestiones, si se modifican las horas de entrada y salida a posteriori no hay rastro de la manipulación, rastro que si quedaría reflejado de ser el registro digital; lo cual no significa que sea imposible de detectar, ya que se podría probar la alteración mediante cámaras en los locales (de estar instaladas legalmente), por las testificales de otros compañeros, etc. Además, otros inconvenientes de este sistema, son las dificultades para los trabajadores que prestan sus servicios fuera del centro de trabajo, la posibilidad de pérdida o destrucción de papel, la mayor complejidad para contar las horas mensuales o anuales de cada trabajador, y su archivo durante cuatro años.

En todo caso, si por parte de los delegados de personal, se negociase este sistema de registro **debe exigirse que en el documento o plantilla que registre la jornada diaria se contengan, como mínimo, los siguientes datos**: los datos del trabajador y de la empresa, el día y la hora de entrada y salida concreta, los descansos entre jornadas en caso de existir, la jornada ordinaria a realizar por el trabajador/a, el detalle de las horas ordinarias, complementarias y extraordinarias desglosadas por cada día de trabajo y la firma del trabajador y del representante legal; debiendo prohibirse que los trabajadores firmen a la vez, la entrada y salida, o que se acumulen los registros para su relleno y firma en fechas posteriores.

Insistimos que resulta dudoso, que este sistema de registro, cumpla con lo dispuesto en la propia Guía del Ministerio de Trabajo, que exige que el documento que registre la hora de entrada y salida tiene que garantizar *la trazabilidad y rastreo fidedigno e invariable de la jornada diaria una vez registrada,* ya que entraña más riesgo de manipulación (tanto a priori como a posteriori) y pérdida o destrucción del registro y, por tanto, debe establecerse que este sistema de registro en soporte papel tiene que garantizar que proporciona una información fiable, inmodificable y no manipulable a posteriori.

En definitiva, teniendo en cuenta el desequilibrio entre las partes en la relación laboral, y la fácil manipulación del soporte papel, deberá verificarse debidamente que los datos que consten en el registro de papel son fiables y ajustados a la realidad de la jornada que realizan las personas trabajadoras.

1.2. SISTEMAS DE REGISTRO CON FICHAJE POR TARJETA O NÚMERO (PIN)

Este sistema de registro, al igual que el anterior, no tiene apenas repercusión en la esfera de la protección de datos ni en la privacidad de la persona trabajadora, y es junto con el sistema de huella digital, de los más utilizados por las empresas. Frente al anterior, es un sistema que garantiza la no manipulación a posteriori y que almacena automáticamente todos los registros de entrada y salida. Sin embargo, para el empresario los principales inconvenientes son el coste de estos sistemas (en caso de no estar implantado ya), que no es apto para aquellos trabajadores cuyo puesto

necesite movilidad o el propio tele-trabajo y el posible fraude en el uso de tarjeta magnética o número pin asignad

2. SISTEMAS DE REGISTRO QUE PRESENTAN MAYOR INCIDENCIA EN LA ESFERA DE LA PROTECCIÓN DE DATOS

2.1. CONSIDERACIONES GENERALES

No cabe duda, que la implantación del registro de jornada está íntimamente relacionada con el uso de las nuevas tecnologías, y de hecho, en una buena parte de las empresas, estas nuevas tecnologías ya se vienen utilizando para el control horario, sin que en algunos casos, se respete la normativa sobre protección de datos. Por tanto, en los sistemas que ahora analizamos, veremos que precauciones han de adoptarse para que estos sistemas de registro cuenten con las debidas garantías en materia de derechos de protección de datos y de intimidad y privacidad de las personas trabajadoras.

Las normas sobre protección de datos en el ámbito laboral se recogen, básicamente en los artículos 20 bis del ET, art. 14.j) bis del Estatuto Básico del Empleo Público, en el RGPD (de aplicación directa en España y cuya regulación, en caso de contradicción, prima sobre la normativa española) y los artículos 87 a 91 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales (LOPDPDG), que regulan el derecho a la intimidad y uso de dispositivos digitales, de sistemas de videovigilancia, de grabación de sonidos y de sistemas de geolocalización en el ámbito laboral. Normativa que habrá de interpretarse teniendo en cuenta la doctrina jurisprudencial sobre esta materia, por parte del Tribunal Europeo de Derechos Humanos, del Tribunal de Justicia de la Unión Europea y de nuestro Tribunal Constitucional.

Por tanto, el empresario, previa negociación colectiva con los RLT, con determinados límites y garantías, que ahora veremos, puede utilizar este tipo de dispositivos digitales y sistemas para el control de la actividad laboral; si bien, en todo caso, las personas trabajadoras tienen derecho a la protección de su intimidad, de tal forma que el acceso y la utilización por el empresario, de los datos obtenidos mediante estos dispositivos o sistemas, respete sus derechos de protección de datos y de intimidad y privacidad.

Desde esta perspectiva el sistema de registro de jornada, en la medida en que pueda suponer el tratamiento de datos de carácter personal, o el acceso a información que comprometa dichos derechos fundamentales como el derecho a la intimidad, deberá ajustarse a los criterios de proporcionalidad y de minimización aplicables por la doctrina del Tribunal Europeo de Derechos Humanos y del propio Tribunal

Constitucional cuando están en juego derechos fundamentales. Como ya extractamos en nuestro anterior documento sobre registro de jornada, la STC 186/2000 resume su doctrina de esta manera: *«la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta con recordar que (como sintetizan las SSTC 66/1995, de 8 de mayo, FJ 5; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero, FJ 8) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes:*

1. *si tal medida es susceptible de conseguir el objetivo propuesto (**juicio de idoneidad**);*
2. *si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (**juicio de necesidad**);*
3. *y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (**juicio de proporcionalidad en sentido estricto**).»*

Partiendo de estas consideraciones generales, veamos los sistemas en cuestión:

2.2. SISTEMAS DE REGISTRO MEDIANTE DISPOSITIVOS DIGITALES (MOVIL, TABLET o PC).

El uso de dispositivos digitales (ordenadores, tablet, móviles, etc) en el ámbito laboral está extendido con carácter generalizado, y por tanto, parece lógico pensar que muchas empresas pretendan utilizar estos dispositivos para el control horario. Además, es un sistema que permite fácilmente "fichar" a los/as trabajadores/as que prestan sus servicios fuera del centro de trabajo o realizan teletrabajo, que apenas tiene coste (si ya se dispone por parte de la empresa de dichos dispositivos) y que permite una buena gestión documental.

No obstante, conviene hacer las siguientes precisiones:

- La primera, y más importante, es que **en ningún caso resulta admisible que las personas trabajadoras tengan que poner a disposición de la empresa sus propios dispositivos** para incorporar el sistema de registro de jornada, por tanto, el trabajador no tiene que utilizar su móvil o dispositivo digital para descargarse la app o aplicación para registrar su hora de entrada o salida.

  En este sentido, se ha pronunciado recientemente la Sentencia de la Audiencia Nacional de 6 de febrero de 209 (en el asunto del proyecto tracker de la

empresa Telepizza), que *considera que la actuación empresarial por la que exige a los trabajadores que aporten el móvil personal, con conexión de datos, para que instalen una aplicación al servicio del control empresarial, es manifiestamente abusiva, pues rompe el principio de ajenidad del contrato de trabajo.*

- En segundo lugar, **debe prohibirse que estos dispositivos digitales activen la geolocalización, salvo en los casos que resulta preciso y necesario, y en este último caso, no podrán activarse permanentemente.**

- En tercer lugar, si bien es cierto, que no se exige consentimiento de las trabajadoras o trabajadores , para establecer este sistema (se encuadraría en el art. 20.3 ET), deberán respetarse **los principios en materia de protección de datos, de proporcionalidad y minimización**, teniendo, además, en cuenta lo dispuesto en el artículo 87 de la LOPD que establece que:

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

- Por tanto, de conformidad con este artículo, para implantar un sistema de registro de jornada que emplee dispositivos digitales han de cumplirse por el **empresario las siguientes <u>garantías</u>[1]:**

[1] Son interesantes en este apartado, entre otras, la Sentencia de 7 de febrero de 2017 del TEDH, (asunto Barbulescu II), la Sentencia de 22 de febrero de 2018 (asunto 2018/35, Libert contra Francia), la Sentencia de la Sala de lo Social del Tribunal Supremo de 8 de febrero de 2018.

1) **Deber de información, a los representantes legales de los trabajadores y a las personas trabajadoras, respecto al uso y finalidad de las tecnologías de control horario; y si el acceso a los datos va a ser utilizado con fines disciplinarios.**

2) **Uso exclusivo de los dispositivos durante la jornada laboral.**

2.3. SISTEMA DE REGISTRO BIOMÉTRICO (HUELLA, RECONOCIMIENTO FACIAL, IRIS..)

2.3.1 CONSIDERACIONES PREVIAS

En cuanto a este tipo de sistemas de registro horario basados en datos biométricos hasta la publicación Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas, eran admitida su utilización como medio de control horario, existiendo además, jurisprudencia que consideraba este sistema como legal y proporcionado (STS de 2 de julio de 2007, entre otras). No obstante, esta conformidad ha de cuestionarse tras la aprobación del Reglamento al estar considerados los datos biométricos como **datos sensibles.**

Según el Reglamento, los datos sensibles son *datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos**, datos biométricos dirigidos a identificar de manera unívoca a una persona física**, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física,* **mereciendo, por ello, una protección especial.** De esta manera, **el RGPD prohíbe su tratamiento con determinadas excepciones**.

Así el apartado b) del art.9.2, señala que no será de aplicación la prohibición general de tratamiento de datos biométricos cuando *"es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado"*.

Por lo tanto, para poder aplicar esta excepción, y tratar datos sensibles, será necesario:

a) Que el tratamiento sea necesario para el cumplimiento de obligaciones o el ejercicio de derechos específicos del empleador o de la persona interesada en el ámbito del derecho laboral o de la seguridad y protección social.

b) Que lo autorice el derecho de la Unión o de los Estados miembros o un convenio colectivo, que establezca garantías adecuadas del respeto de los derechos fundamentales y los intereses de las personas afectadas.

Pues bien, en materia de registro de jornada, el primer requisito, necesidad de cumplimiento de obligaciones en materia laboral, se cumple, puesto que existe una obligación legal de garantizar el registro diario de jornada impuesta en el art. 34.9 del ET. Sin embargo, en cuanto a la segunda condición impuesta, autorización de su tratamiento por el derecho comunitario, nacional o convenio colectivo, de la lectura de la legislación española, no se deduce claramente la posibilidad de utilización de datos biométricos en un sistema de registro de jornada.

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

Por su parte, el art 20.bis del ET, se refiere a dispositivos digitales, videovigilancia y geolocalización, estableciendo que *los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.*

Y finalmente, los artículos 87, 89 y 90 de la LOPDDG, han previsto y regulado únicamente las condiciones y garantías con las que puede hacerse el control de los trabajadores por parte del empresario con respecto a la utilización de los dispositivos digitales puestos a su disposición por parte del empresario, la utilización de sistemas de videovigilancia en el puesto de trabajo o la utilización de sistemas de geolocalización en el ámbito laboral, pero no contienen referencia alguna a los datos biométricos.

Por ello**, salvo que por convenio colectivo**, a través de los cauces de la negociación colectiva, y siempre, en este caso, con respeto a las garantías exigidas en el RGPD y LOPDGDD, que seguidamente se detallaran, se acordara implantar sistemas de registro biométricos, puede concluirse a nuestro juicio, que **no existe una norma con rango de ley, que autorice la utilización de datos biométricos para los controles de la jornada laboral.**

En este sentido se ha pronunciado la Agencia Catalana de Protección de Datos en su reciente Dictamen CNS 63/2018.

Sin perjuicio de lo señalado, y para los supuestos en los se pueda plantear una negociación con los representantes legales de los trabajadores para implantar estos sistemas, o en los casos en los que ya estén implantados en las empresas (lo cual exige una renegociación de este sistema de control horario para ver si se acomoda a la normativa de protección de datos), conviene especificar qué **garantías deben de**

cumplirse para que se considerara legal y proporcionado la obligación de registro con un sistema tan invasivo del derecho de intimidad de los trabajadores, como es el tratamiento de datos biométricos.

2.3.2 PRINCIPIOS Y GARANTIAS EN EL TRATAMIENTO DE DATOS PERSONALES SENSIBLES.

- **PRINCIPIO DE MINIMIZACIÓN**

El nuevo Reglamento recoge 6 principios: el **de minimización de datos**, de limitación de la finalidad, de exactitud, de limitación del plazo de conservación, de seguridad y finalmente el de transparencia. En concreto, el artículo 5 señala que, los datos personales serán:

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

*b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («**limitación de la finalidad»);***

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

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

*e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado **(«limitación del plazo de conservación»);***

*f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («**integridad y confidencialidad**»).*

Teniendo en cuenta estos principios **y sobre todo el principio de minimización (y proporcionalidad),** el propio Consejo de Ministros del Consejo de Europa en una Recomendación del año 2015, sobre el tratamiento de datos personales en el contexto laboral (principio 18) fijo que:

"18.1 La recopilación y posterior procesamiento de los datos biométricos ***solo se deberían emprender cuando hay que proteger los intereses legítimos de empresarios, empleados o terceros, solo si no hay otros medios menos intrusivos disponibles*** *y solo si se acompaña de las garantías adecuadas previstas en el principio 21. 18.2. El tratamiento de los datos biométricos se debe basar en métodos científicamente reconocidos y debe estar sujeto a los requisitos de estricta seguridad y proporcionalidad*". Igualmente, el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29, señala que "*Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado".*

Por tanto, atendiendo al principio de minimización, los RLT a la hora de negociar los sistemas de registro, deben optar por otros sistemas de control menos invasivos, que sin utilizar y tratar categorías de datos especialmente protegidos, como los biométricos, puedan permitir alcanzar la misma finalidad. No queda amparado el uso de este tipo de sistemas por el hecho de que resulte más barato o fiable, porque es evidente que la utilización de sistemas biométricos para registrar la jornada puede evitar el riesgo de suplantación que puede producirse en algún caso, pero ello, no justifica, de ningún modo, su utilización.

El Dictamen de la Agencia Catalana pone de manifiesto que algunas Autoridades Europeas de Protección de Datos, como la francesa o la italiana, no han admitido la utilización de sistemas de control basados en datos biométricos como sistema generalizado de control horario de los trabajadores por parte del empresario.

Por ello, solamente, entenderíamos que en función de determinados riesgos existentes, o por las peculiaridades de los servicios que los trabajadores presten (piénsese en centros de trabajo o instalaciones que deben contar con una restricción importante de acceso, defensa, seguridad, centrales nucleares, etc), podría ser adecuado y proporcional implantar un sistema biométrico de control horario, con las garantías que señalamos:

a) INFORMACION A LOS RLT Y TRABAJADORES

En relación con el derecho de información previa de los RLT como de las personas trabajadores, tanto el art. 64.5 ET, como la normativa en materia de protección de datos (LOPD –art.11, y 87 a 90- y RGPD) determinan que el empresario deberá negociar su implantación, explicando e informando la necesidad, adecuación, motivos y conveniencia de implantar este sistema, garantizando que no existe otro método más moderado y respetuoso con el derecho de intimidad de las personas trabajadoras para conseguir la misma finalidad, el control horario (principio de minimización y proporcionalidad). Además, se deberá informar expresamente de la imposibilidad, por parte de la empresa, para tratar los datos con otros fines que no sea el registro de jornada.

b) IDONEIDAD Y PROPORCIONALIDAD EN EL PROPIO SISTEMA BIOMETRICO

En caso haberse acreditado la necesidad de su implantación, que como hemos visto, tiene que superar el principio de minimización, asegurando que no es posible implantar otro sistema de registro menos invasivo, las garantías adicionales, señaladas por la propia Agencia de Protección de Datos, que deben aplicarse para proteger el tratamiento de esos datos son:

- **Cifrado** de los datos.
- **Almacenar esos** datos biométricos en sistemas no centralizados, incorporando los mismos a una tarjeta inteligente en poder del usuario.
- Diseño del sistema que permita **revocar el vínculo de identidad.**
- **Imposibilidad** de interconexión de la base de datos biométricos con otras bases.

2.4 SISTEMA DE REGISTRO DE GEOLOCALIZACIÓN[2]

La geolocalización (o localización por satélite), es un sistema que se incorpora a los móviles, pulseras, vehículos, u otros dispositivos, y que permite a la empresa conocer la posición exacta del empleado en tiempo real, y por lo tanto controlar la prestación de servicios en un horario y lugar determinado; siendo, muy empleado en aquellos sectores de actividad donde la prestación de servicios se realiza fuera del centro de trabajo.

Esta recogida de **datos de localización de las personas trabajadoras es, según dispone el art. 4.1) del RGPD un dato personal**, y por tanto, conforme con el art. 4.2 del

[2] Sobre sistemas de geolocalización mencionar la reciente Sentencia de la Audiencia Nacional de 6 de febrero de 2019, estimada a CCOO en un conflicto colectivo, en el que se declara nulo el proyecto tracker (basado en un sistema de geolocalización) de la empresa Telepizza por vulnerar la normativa sobre protección de datos, también es interesante la Sentencia de 2 de septiembre de 2010 del TEDH (caso Uzun contra Alemania), la Sentencia del TSJ Pais Vasco de 2 de julio de 2007, de Castilla la Mancha de 29 de junio de 2017, entre otras. Así, por ejemplo, se considera inválido el control de una trabajadora por GPS fuera de su jornada laboral, pues únicamente ha sido informada de que su vehículo dispone de un control de geo-posicionamiento, cuyo objeto es "garantizar la seguridad y coordinación de los trabajos", siendo impertinente la vigilancia realizada durante los fines de semana y también durante una baja laboral.

mismo cuerpo legal, cualquier operación que se efectúe sobre los mismos tiene el carácter de "tratamiento"; en consecuencia, el mismo exige respetar toda la normativa europea y nacional sobre protección datos. De tal forma, que si no se cumplen las garantías adecuadas y no se imponen límites a su tratamiento, se vulnera el derecho de intimidad y privacidad de la persona protegido por el art. 18, 1 y 4 de la CE.

La normativa en protección de datos (LOPDPDG) dispone que:

Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. ***Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos.*** *Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.*

Por tanto, la implementación de este sistema de requiere:

a) En primer lugar, al igual que cualquier otro tipo de sistema de registro, **se requiere la negociación con los RLT.**

b) En segundo lugar, respeto al **principio de minimización y proporcionalidad,** como señala el Grupo de Trabajo del Artículo 29 (RGPD), en su Dictamen 13/2011, sobre los servicios de geolocalización en los dispositivos móviles inteligentes *"el empresario debe siempre buscar los medios menos intrusivos, evitar un seguimiento continuo y, por ejemplo, elegir un sistema que envíe una alerta cuando un empleado cruce una frontera virtual preestablecida. El empleado deberá poder desactivar cualquier dispositivo de vigilancia fuera de las horas de trabajo y deberá instruírsele sobre cómo hacerlo".* Por tanto, el sistema elegido debe ser el menos invasivo, entre los posibles y con el único fin del control horario, de lo contrario, cabría concluir que hay una lesión de un derecho fundamental de intimidad y privacidad.

Por su parte , la Agencia de Protección de Datos, en su Informe 193/2008 establece que los datos obtenidos a través del sistema de geolocación (rutas seguidas, tiempos de parada, velocidad, consumo de combustible del vehículo, horas de funcionamiento, etc.) son datos de carácter personal, merecedores, en consecuencia, de toda la protección y garantías establecidas en materia de protección de datos, recordando también que el Grupo de Trabajo del art. 29 ha dejado claro que "*habida cuenta de la obligación de que se traten los datos para*

fines específicos, el tratamiento de datos de localización relativos a empleados ha de corresponder a una necesidad específica de la empresa que guarde relación con su actividad. El tratamiento de los datos de localización ha de estar justificado si se lleva a cabo formando parte del control del transporte de personas o bienes o de la mejora de la distribución de los recursos para servicios en puntos remotos (por ejemplo, la planificación de operaciones en tiempo real) o cuando se trate de lograr un objetivo de seguridad en relación con el propio empleado o con los bienes o vehículos a cargo. Por el contrario, el tratamiento de datos es excesivo en caso de que los empleados puedan organizar libremente sus planes de viaje o cuando se lleve a cabo con el único fin de controlar el trabajo de un empleado, siempre que pueda hacerse por otros medios"

c) I**nformación previa, expresa, clara e inequívoca** (los arts. 12 y 13 del RGPD, art. 11 y 90 LOPD)**,** en la que deberá constar, como mínimo:

- el sistema de geolocalización que se va a implantar,
- a partir de qué fecha,
- que información se va a obtener con esa geolocalización,
- garantizar e informar que sólo y exclusivamente va a funcionar durante la jornada laboral, siendo inadmisible su uso fuera de la jornada laboral, aunque el dispositivo sea propiedad del empleador.
- la finalidad con la que se recogen los datos (exclusivamente control horario),
- donde se van a almacenar los datos,
- quien los vas a tratar;
- y finalmente garantizar que la persona trabajadora tiene derecho a acceder, rectificar, limitar o cancelar los datos referentes a su persona incluidos en ese fichero.