Expediente Nº: E/02689/2012

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad ***CONTENUR, S.L..*** en virtud de denuncia presentada por D. ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 14 de febrero de 2012, tuvo entrada en esta Agencia escrito de D. ***A.A.A.*** (en lo sucesivo el denunciante) en el que denuncia a la compañía **CONTENUR, S.L.**. manifestando que la empresa ha instalado un dispositivo de posicionamiento global (G.P.S.) en el vehículo que utiliza para desempeñar su trabajo sin haber sido informado al respecto, según establece el artículo 5 de la Ley Orgánica 15/1999, lo cual puede vulnerar sus derechos.

Añade que tuvo conocimiento de los hechos el día 7 de febrero de 2012 durante una reunión personal con encargados de dicha compañía y posteriormente en una reunión con colaboradores de la misma.

Se adjunta con la denuncia escrito remitido por la sociedad Contenur al denunciante, con fecha de **9 de febrero de 2012**, en el que le informan de lo siguiente:

"Por medio de la presente le comunicamos la decisión de esta empresa de proceder, en virtud de lo dispuesto en el artículo 62 del XV Convenio General de la Industria Química de aplicación, a la apertura de expediente contradictorio por la posible comisión de una falta muy grave de fraude, deslealtad o abuso de confianza en las gestiones encomendadas, prevista en el artículo 6.4 del citado Convenio, que podría ser merecedora incluso de la sanción de despido.

*Los hechos que se le imputan son los siguientes: Que siendo sus funciones (…) y teniendo Vd. asignado para dicha función el vehículo de la empresa matrícula ****, dotado de un sistema de localización permanente mediante un dispositivo G.P.S., tras comprobar el contenido de sus partes de trabajo correspondientes a los días 23, 24, 25, 26, 27, 30 y 31 de enero y cotejarlo con los datos de localización, trayectos, paradas y tiempos empleados obtenidos del dispositivo G.P.S. (…)".*

Se adjunta *Informe de Arranques y Paradas* de fecha **23 de enero de 2012** en el que consta una relación con la siguiente información: *hora-dirección inicial, hora-dirección final, duración, distancia, velocidad y parado (h:m*).

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. En el Registro General de Protección de Datos se encuentra inscrito el fichero denominado “Recursos Humanos”, cuyo responsable es la compañía Contenur, S.L. y entre los datos de carácter identificativo que incluye se encuentra “*matrícula vehículo, geolocalización*

2.La empresa Contenur, S.L. ha comunicado a la Inspección de Datos, con fecha de 14 de septiembre de 2012, en relación con la instalación de un dispositivo G.P.S. en el vehículo utilizado por el denunciante lo siguiente:

- La compañía ha procedido al cumplimiento del deber de información al denunciante para el cumplimiento del artículo 5 de la Ley Orgánica 15/1999, por dos vías independientes:

Por “escrito” a través de la *Política de Privacidad para Personal Interno* que fue firmada por el trabajador el día 15 de diciembre de 2009. En dicho documento se informa de diversos aspectos contemplados en la Ley Orgánica 15/199, como la finalidad del tratamiento de los datos personales del trabajador, las cesiones y el procedimiento para ejercer los derechos.

De forma “verbal” por medio de dos reuniones informativas dirigidas a todos los trabajadores afectados por la instalación de los dispositivos de geolocalización, con fecha de 2 de septiembre y de 19 de octubre de 2011. Para el conocimiento de dichas reuniones por parte del personal se publicó un cartel informativo en el tablón del centro en los días previos a que tuviera lugar.

En las Actas consta que asistió a la reunión el denunciante y se informaron, entre otros, de los siguientes temas “*G.P.S.: se están colocando G.P.S. en los vehículos de Iglus, también en el resto de servicios, esto es debido a la detección de incidencias en las contratas habituales (…)*” y “*G.P.S.: es necesario informar de la instalación: hecho en otras reuniones, los datos al estar relacionados con contrato laboral, no es necesario consentimiento del trabajador para su uso, es necesario informar de la implantación, solo durante la jornada laboral, vehículo de la empresa (…)”.*

También, el Presidente del Comité de Empresa confirma las citadas convocatorias según consta en la declaración firmada por él mismo.

Se aporta copia de las Actas, del cartel informativo de la reunión del 19 de octubre de 2011 y la declaración del Presidente del Comité de Empresa.

- Los dispositivos G.P.S. fueron instalados en la segunda y tercera semana del mes de noviembre de 2011 y continúan en uso en la actualidad. La información registrada por dichos equipos se mantiene activa durante dos meses transcurridos los cuales se conserva bloqueada y con acceso restringido. El acceso a los datos personales está restringido a los encargados y jefes del Departamento de Contratas y son los siguientes: matrícula del vehículo, coordenada de la posición y hora, velocidad, estado del motor arrancado o parado y odómetro (contador de metros). Dichos datos almacenados en el sistema G.P.S. se encuentran asociados a un código que únicamente desde Contenur se puede vincular al nombre y apellidos del trabajador.

- La finalidad de dichos dispositivos es el control del cumplimiento de las funciones y obligaciones de los conductores durante la jornada laboral, así como la detección de posibles incidencias durante la conducción, en ejercicio de la potestad de dirección y

control de la actividad laboral que el Estatuto de los Trabajadores establece en su artículo 20. Adicionalmente el sistema permite la localización de vehículos robados.

Tras la instalación de los equipos se detectaron varios incumplimientos del artículo 61.4 del XV Convenio General de la Industria Química por parte del denunciante que supuso la imposición de una sanción muy grave

- Añade la compañía que, además, la instalación de los equipos G.P.S. es una exigencia de sus clientes para la prestación de un correcto servicio y para que dispongan de herramientas que puedan demostrar y confirmar la ejecución de los trabajos contratados.

En ningún caso los clientes de Contenur tienen acceso a los datos del sistema ya que la herramienta permite disociar la información

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

La LOPD en su artículo 6, recoge:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento";

En el presente caso, esta probada la relación laboral del denunciante con la empresa denunciada, Contenur S.L.

El Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores –ET- ha atribuido facultades específicas a la empresa que posibilitan el control del desarrollo de la prestación laboral y el ejercicio de estas facultades comporta en muchas ocasiones tratamientos de datos personales. Su artículo 20, apartado 3 y 4 , disponen:

«3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

4. El empresario podrá verificar el estado de enfermedad o accidente del trabajador

que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones. (Art. 20.3 y 4 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores).

Cuando para el desarrollo de la función empresarial de control se utilizan las tecnologías de la información, las posibilidades de repercusión en los derechos del trabajador se multiplican y se manifiestan de muy diversos modos.

Pueden citarse entre otros, los controles biométricos como la huella digital, la videovigilancia, los controles sobre el ordenador, -como las revisiones, el análisis o la monitorización remota, la indexación de la navegación por Internet, o la revisión y monitorización del correo electrónico y/o del uso de ordenadores-, **o los controles sobre la ubicación física del trabajador mediante geolocalización.**

En la mayor parte de estos supuestos existen tratamientos de datos personales y, en consecuencia es necesario cumplir con los principios de protección de datos. La Agencia Española de Protección de Datos y la jurisprudencia de los tribunales han venido indicando distintos supuestos en los que tales tratamientos son admisibles y las condiciones para su realización.

Por otro lado, el uso de tecnologías de la información multiplica las posibilidades de control empresarial y obliga a tener en cuenta el respeto a los derechos fundamentales de los trabajadores, a adoptar medidas de control que sean proporcionales y respeten su dignidad, su derecho a la protección de datos y su vida privada.

Existe por tanto, un conjunto de principios cuyo respeto resulta recomendable cuando no prácticamente ineludible.

La legitimación para el tratamiento deriva de la existencia de la relación laboral y, por tanto, de acuerdo con el trascrito artículo 6.2 LOPD, no se requiere del consentimiento.

A la hora de decidir adoptar una medida de control que comporte un tratamiento de datos personales debe aplicarse el principio de proporcionalidad, así puede ser perfectamente razonable dotar de un dispositivo de geolocalización en tareas como el transporte de mercancías para las que resulte relevante conocer donde se encuentra el vehículo y en qué momento podrá realizar una determinada entrega. Ello no puede suponer que se facilite un dispositivo de esta naturaleza a todos los trabajadores de la empresa cuando su tipo de prestación no lo haga necesario.

Debe existir una “finalidad” que, en este caso, no puede ser otra que la establecida por el trascrito artículo 20.3 ET de *«verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales»*.

« En cuanto a la posibilidad de que las huellas sean tratadas sin consentimiento del interesado, (...) será posible el tratamiento inconsentido, ya que el artículo 6.2 de la LOPD prevé que no será preciso el consentimiento cuando los datos "se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento" (Informe sobre Tratamiento de la huella digital de los trabajadores)»

Los datos que se obtengan y almacenen deberán ser exactos y puestos al día y no podrán conservarse más tiempo del necesario. Se recomienda a los empleadores fijar un plazo de conservación.

Debe cumplirse con el deber de "información" a los trabajadores. Este deber resulta particularmente relevante cuando se trate de controles sobre el uso de Internet y/o del correo electrónico. En este caso es muy recomendable que la información a los trabajadores sea clara en lo que respecta a la política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales. Así como que incluya la finalidad de la vigilancia, y cuando pueda repercutir sobre medios que el trabajador utiliza normalmente una información sobre las medidas de vigilancia adoptadas.

Por otra parte, en la medida en la que este tipo de controles inciden sobre el conjunto de la empresa puede ser muy recomendable informar también a los representantes de los trabajadores de las políticas adoptadas en esta materia. No se trata en absoluto de que el trabajador conozca el detalle de políticas de seguridad que pueden afectar a ámbitos que la empresa necesita proteger. Sin embargo, es indispensable que conozca por ejemplo si puede recibir mensajes privados, o depositar fotografías en determinados espacios en su ordenador o en un servidor corporativo.

La información previa y su prueba es esencial, ya que estos tratamientos no requieren el consentimiento del trabajador y son manifestación de los poderes de control del empresario.

«..es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos. (Sentencia de la Sala de lo Social del Tribunal Supremo de 26 de septiembre de 2007)».

En síntesis, el Tribunal Supremo en la Sentencia de fecha 26 de septiembre de 2007 sobre el *"control empresarial del correo electrónico",* concluye la posibilidad de que el empresario pueda acceder al control del ordenador, del correo electrónico, los accesos a Internet de los trabajadores y a controles de geolocalización , siempre que la empresa de *"buena fe"* haya establecido *"previamente"* las reglas de uso de esos medios con aplicación de prohibiciones absolutas o parciales e informado de que va existir un control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos.

III

Pues bien, de las diligencias preliminares llevadas a cabo por la Inspección, se desprende que la empresa denunciada informó de buena fe y previamente a los trabajadores s de la instalación de GPS en los vehículos de la empresa, conducta que observa las prescripciones previstas en la normativa sobre protección de datos y jurisprudencia consolidada, por lo que procede el archivo de las actuaciones

El Real Decreto 1720/2007, de 21 de siembre, por el que se aprueba el reglamento de desarrollo de la LOPD en su artículo en su artículo 94.4 recoge:

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a ***CONTENUR, S.L..*** y a ***A.A.A..***

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

José Luis Rodríguez Álvarez

Director de la Agencia Española de Protección de Datos