Expediente Nº: E/02994/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha 22 de abril de 2013, tuvo entrada en esta Agencia escrito de D. ***A.A.A.*** (en lo sucesivo el denunciante) en el que denuncia a la mercantil ***PROSEGUR COMPAÑIA DE SEGURIDAD, S.A.*** en Cantabria (en adelante PROSEGUR) que tiene, entre sus clientes, al Centro de Proceso de Datos -CPD-del Banco de Santander para la prestación de servicios de seguridad, expone que los empleados de PROSEGUR que prestan servicios para el CPD deben aportar los datos de: nombre y apellidos, DNI, dirección particular, número de teléfonos particulares, lugar de nacimiento, categoría profesional, nº de tarjeta profesional, servicio asignado, fecha de alta en la empresa y estudios y cursos formativos profesionales, para que estén a disposición de los responsables de PROSEGUR.

Añade que, con fecha 9 de enero de 2013, PROSEGUR entregó a cada trabajador un documento informativo sobre normas de utilización del teléfono móvil particular durante la jornada laboral y en marzo de 2013, dicha entidad sancionó a 21 vigilantes de seguridad adscritos al servicio de seguridad del CPD del Banco de Santander por la utilización del teléfono móvil particular para usar el "*whatsapp"* especificando fecha y hora de utilización.

El denunciante, también, manifiesta que para poder especificar la utilización del teléfono móvil en las dependencias del cliente, PROSEGUR les ha facilitado el fichero con datos personales de los empleados ya que, según ha manifestado PROSEGUR a los representantes sindicales de los trabajadores, éste ha utilizado un sistema de comprobación de uso del whatsapp. Asimismo manifiesta que PROSEGUR en ningún momento ha solicitado el consentimiento para la comunicación de sus datos personales al cliente y para la el acceso a la información privada del uso del móvil particular.

Adjunto a la denuncia, se ha aportado, entre otra documentación, fotografías del comunicado de la empresa, de fecha 9 de enero de 2013, indicando que no se permite el uso del teléfono móvil y copia de uno de los escritos de sanción.

SEGUNDO: Con fecha 22 de mayo de 2014, el director de la AEPD dictó resolución de Caducidad de Actuaciones Previas de Investigación declarando caducadas las actuaciones de investigación, E/3304/2013, e iniciando nuevas actuaciones E/02994/2014.

TERCERO: Por la Subdirección General de Inspección de Datos se ha procedido a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Tal y como consta en la documentación remitida por PROSEGUR con fechas de registro de entrada a esta Agencia 12 de diciembre de 2013, 24 de enero de 2014 y 12 de junio de 2014:

1. PROSEGUR tiene suscrito un contrato de arrendamiento de servicios con SANTANDER GLOBAL FACILITIES, SLU, de fecha 14 de noviembre de 2011, cuyo objeto es la prestación al CPD del Banco de Santander de un servicio de seguridad consistente en Vigilantes de Seguridad armados en servicio de 24 horas y con capacidad de radioscopia básica, conocimientos de ofimática, y manejo de ordenadores y monitores cuadrantes.
2. En virtud de este contrato, el personal de PROSEGUR debe prestar sus servicios en las instalaciones del Banco de Santander, al objeto de dotar de seguridad a las instalaciones objeto de protección, lo que conlleva que el titular de la instalación conozca ciertos datos de carácter personal del personal de PROSEGUR que va a prestar sus servicios en sus instalaciones. Por ello, PROSEGUR comunica los datos personales de sus empleados que prestan allí sus servicios: Nombre y Apellidos, Número de DNI, Número de T.I.P, Número de la Seguridad Social, Número de teléfono de contacto, Domicilio, Fecha de nacimiento, Formación académica y complementaria e Historial laboral.
3. PROSEGUR manifiesta que el CPD del Banco Santander es considerado como un centro de alta seguridad, donde se deben extremar las medidas de seguridad incluidas aquellas que supongan utilización de medios técnicos que puedan comportar la extracción de información de dichas instalaciones.

   A este respecto, el denunciante ha aportado fotografía del comunicado por el que se restringe el uso de teléfonos móviles personales o aparatos análogos, de fecha 9 de enero de 2013 y donde se indica los teléfonos a utilizar para caso de necesidad.

   *"**Comunicado Interno**, Asunto Uso del teléfono Móvil, fecha 9/01/2013; Texto: Por el presente se pone en conocimiento que a partir de la fecha, no se permitirá el uso del teléfono particular (o aparatos análogos) en el puesto de trabajo, por lo que se recomienda no lo porten para evitar mal entendidos. En el CTC hay un teléfono 24 horas que deberán dar a quien estimen oportuno para casos urgentes y necesidad."*

   *"**Comunicado Interno**, Asunto Uso del teléfono móvil, fecha 9/01/2013 de forma complementaria al comunicado interno entregado por la empresa sobre la prohibición del uso del teléfono en el puesto de trabajo, se asignan los siguientes números de teléfonos, los cuales se han facilitado para que llamen en caso de necesidad o urgencia o para contactar con los vigilantes que estén prestando servicio."*

4. Respecto de la forma en que PROSEGUR ha tenido conocimiento del acceso a la aplicación de "*whatsapp"* de algunos de sus empleados tal y como consta en el documento de sanción aportado por el denunciante, ésta manifiesta que:

   No dispone de ningún dispositivo o sistema que le permita verificar la utilización de los teléfonos móviles de sus empleados o de cualquier aplicación que en los mismos pudieran tener.

Para el desarrollo del servicio contratado, PROSEGUR estableció la correspondiente cadena jerárquica, por la cual existe un responsable del servicio en cada turno de trabajo, que se encarga, además de desempeñar las funciones propias de su cargo, de que el servicio sea prestado en las condiciones contratadas.

Los teléfonos particulares de cada empleado son de su exclusiva titularidad y PROSEGUR en ningún momento ha utilizado ni utiliza dispositivos que puedan controlar de alguna forma la utilización de los mismos pero el Coordinador de Servicios, a través de su propio teléfono móvil, pudo comprobar cómo algunos trabajadores de la compañía habían accedido por última vez a la aplicación de "*whatsapp"*, ya que esta aplicación es de pública difusión y en la misma aparece la última vez que se ha accedido al programa con sólo seleccionar al usuario deseado.

No se han aplicado sistemas de intrusión, ni se han utilizado datos que no sean de público conocimiento y difusión, ya que la propia aplicación "*whatsapp"* que es pública se encarga de difundir en qué hora y día se ha realizado el último ingreso de cada usuario en la misma.

PROSEGUR ha aportado fotocopia de un terminal móvil donde figuran el nombre de usuario y la fecha y hora de accesos a la aplicación "*whatsapp",* las cuales, según sus manifestaciones corresponde con los trabajadores de su compañía sancionados.

No obstante, aunque la aplicación de "*whatsapp"* informa del usuario y de la última hora de acceso a la aplicación no se puede acreditar que la persona que ha accedido sea el titular de la línea ya que "*whatsapp",* no solicita ningún sistema de identificación y autenticación del usuario para acceder.

5. Respecto de la información que se ha facilitado a sus empleados con respecto a la posible utilización por parte de la empresa de los accesos realizados utilizando la aplicación de "*whatsapp"* con la finalidad de posibles sanciones, PROSEGUR manifiesta que la persona que puso en conocimiento de la empresa qué trabajadores habían participado en una conversación a través del "*whatsapp"* era un miembro de esa conversación. PROSEGUR manifiesta que no monitoriza ni controla los dispositivos electrónicos personales de sus trabajadores por lo que no se pudo informar previamente de alguno que no ha tenido intención de realizar.
6. Respecto del consentimiento otorgado por sus empleados para el acceso a la información del teléfono móvil particular, PROSEGUR manifiesta que no existe consentimiento otorgado por los trabajadores para el acceso a los teléfonos móviles particulares, dado que PROSEGUR no accede a los mencionados dispositivos de ninguna forma.

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

El denunciante expone, de un lado la *cesión* de los datos de los trabajadores sin su consentimiento desde la entidad Prosegur a su cliente Banco de Santander y, de otro lado haber accedido a la aplicación de *whatsapp* de los teléfonos móviles particulares de los vigilantes de PROSEGUR para fundamentar 21 expedientes disciplinarios de los vigilantes que prestan servicios en el CPD del Banco Santender.

La LOPD en su artículo 11, recoge:

"2. El consentimiento exigido en el apartado anterior no será preciso: c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique".

Y el artículo 12, prevé:

"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento".

En el caso analizado, PROSEGUR suscribió un contrato de *arrendamiento de servicios* del transcrito articulo 12 con Santander Global Facilities SLU, de fecha 14 de noviembre de 2011, cuyo objeto es la prestación al CPD del Banco de Santander de un servicio de alta seguridad con vigilantes de seguridad armados en servicio de 24 horas y con capacidad de radioscopia básica, conocimientos de ofimática, y manejo de ordenadores y monitores cuadrantes, debiendo prestar sus servicios en las instalaciones del Banco de Santander al objeto de dotar de seguridad a las instalaciones objeto de protección, que justifica la *cesión* y que el titular de la instalación (B. Santander) conociera ciertos datos de carácter personal del personal de PROSEGUR que va a prestar sus servicios en sus instalaciones como eran: el nombre y apellidos, el número de DNI, el número de T.I.P, el número de la Seguridad Social, el número de teléfono de contacto, el domicilio, la fecha de nacimiento, la formación académica y complementaria y el historial laboral.

Por tanto, la comunicación de los relacionados datos de los vigilantes de seguridad al responsable de las instalaciones del CPD del banco de Santander en Cantabria no exige el consentimiento de los afectados para la comunicación al estar amparados en el artículo 11 y 12 de la LOPD n, por otra parte consta la oposición de loa afectados.

III

Respecto a la segunda de las cuestiones planteadas, esto es que PROSEGUR se valió de la comprobación del uso de la aplicación whatsapp de los teléfonos móviles de los vigilantes para fundamentar los 21 expedientes disciplinarios y no fueron informados debidamente de dicha posibilidad, se ha de señalar que de la inspección documental realizada por el personal inspector de esta Agencia en el período de "diligencias previas", pueden diferenciarse dos acciones, de una parte la constitución del "grupo" whatsapp entre los vigilantes del CPD y el correspondiente supervisor en la que no se desprende intervención del empresario PROSEGUR y, de otra el acceso probado a la información del whatsapp y el uso en los expedientes disciplinarios por dicha entidad, información y uso que lleva a valorar su legalidad desde el punto de vista de protección de datos.

IV

El Reglamento de la LOPD en su artículo 4, recoge:

"El régimen de protección de datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:: a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domesticas"

La creación de un "grupo" en la aplicación whatsapp entre los vigilantes de PROSEGUR del CPD se ha considera como un caso de actividad "personal" o de "exención doméstica" a la que es ajena PROSEGUR al no constar indicio de su intervención. Es así, puesto que la creación del "grupo" responde: a una acción concertada entre los vigilantes y el respectivo supervisor; a que los números de teléfonos móviles facilitados eran particulares no proporcionados por la empresa no siendo susceptibles todos los terminales de la instalación de la referida aplicación; a que los afectados no podían ignorar, al ser de general conocimiento, la incorporación automática al grupo con solo añadir al terminal el nº de teléfono móvil de la persona que es usuario de dicha aplicación; y a que el hecho de que por su especificidad laboral tuviesen que facilitar el nº de teléfono no comporta la finalidad del control de la aplicación whatsapp que no es instalable en todos los terminales.

PROSEGUR ha asegurado sin que pueda ser contradicho que no dispone de ningún dispositivo o sistema que le permita verificar la utilización de los teléfonos móviles de sus empleados o de cualquier aplicación que en los mismos pudieran tener.

La AEPD en su resolución de 21 de octubre de 2014, E/03943/2014, analizando una denuncia en que el denunciante accede a la difusión a través del whatsapp de su teléfono privado de comentarios despectivos sobre él a los participantes del "grupo", recoge: *<<El Grupo de Trabajo del artículo 29 (GT29), órgano consultivo europeo independiente establecido en virtud del artículo 29 de la Directiva 95/46/CE, adoptó el 12 de junio de 2009 el Dictamen 5/2009, sobre las redes sociales en línea. Este documento se centra en cómo el funcionamiento de los servicios de redes sociales (SRS) puede satisfacer los requisitos de la legislación sobre protección de datos de la Unión Europea.* ***En particular, en el documento se destaca cómo muchos usuarios de las redes sociales se mueven dentro de una esfera puramente personal, poniéndose en contacto con gente como parte de la gestión de sus asuntos personales, familiares o domésticos****. Según destaca el GT29, la citada Directiva* ***no impone las obligaciones de un responsable de datos a un individuo que procesa datos personales "en el transcurso de actividades estrictamente personales o domésticas"****. Siguiendo este precepto, el GT29 estima que, con carácter general, en la mayor parte de las actividades realizadas por los usuarios de un SRS debe aplicarse lo que denomina "exención doméstica", en lugar de la normativa de protección de datos>>.*

V

La segunda cuestión, es la concerniente al acceso y utilización de la información de la aplicación whatsapp por la entidad PROSEGUR para fundamentar 21 expedientes disciplinarios, que lleva a determinar el cumplimiento del artículo 5 de la LOPD requisito previo al tratamiento de la información así como de la finalidad del uso de dicha información a efectos laborales, en cuanto supone la intromisión en la intimidad de una herramienta particular del trabajador, partiendo de la premisa de que dicha información fue suministrada a la entidad por el supervisor de los vigilantes del CPD.

El artículo 6 de la LOPD exige, como norma general, el consentimiento del afectado para el *"tratamiento"* de sus datos, salvo que se encuentre exceptuado por alguna de las causas recogidas en sus apartados 1 y 2, esto es, que lo disponga una *"Ley"* o *"los datos de carácter personal 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".*

Por su parte, el artículo 5 de la LOPD se refiere al derecho de información, en el sentido siguiente:

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

La doctrina del Tribunal Supremo en su Sentencia de 26/09/2007 sobre el control empresarial de las herramientas puestas a disposición del trabajador, exige, en síntesis, que las restricciones que se establezcan por el empresario sobre el uso de las herramientas del empresario informe de buena fe, de forma clara y previamente de las restricciones al uso de herramientas informáticas en el desempeño de sus funciones laborales y sus consecuencias, siendo dicha obligación extensible a la restricción establecida previamente por el empresario para la utilización del teléfono móvil del trabajador en el puesto de trabajo.

En el presente caso, el denunciante ha aportado fotografías de los comunicados de fecha 9 de enero de 2013 de PROSEGUR, por los que se restringe el uso del teléfono móvil personal y se indica los teléfonos de la empresa a utilizar para caso de necesidad, con el siguiente tenor:

*"**Comunicado Interno**, Asunto Uso del teléfono Móvil, fecha 9/01/2013; Texto: Por el presente se pone en conocimiento que a partir de la fecha, no se permitirá el uso del teléfono particular(o aparatos análogos) en el puesto de trabajo, por lo que se recomienda no lo porten para evitar mal entendidos. En el CTC hay un teléfono 24 horas que deberán dar a quien estimen oportuno para casos urgentes y necesidad."*

*"**Comunicado Interno**, Asunto Uso del teléfono móvil, fecha 9/01/2013 de forma complementaria al comunicado interno entregado por la empresa sobre la prohibición del uso del teléfono en el puesto de trabajo, se asignan los siguientes números de teléfonos, los cuales se han facilitado para que llamen en caso de necesidad o urgencia o para contactar con los vigilantes que estén prestando servicio."*

Con independencia de la existencia de la relación contractual entre PROSEGUR y los vigilantes que prestan servicios en el CPD del Banco Santander, el Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el Texto Refundido 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 *"Dirección y Control de la Actividad Laboral"*, 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, siendo ello aplicable

tanto a la utilización de herramientas puestas a disposición por el empresario como, por analogía, a la utilización del teléfono móvil particular por el trabajador siempre que la limitación impuesta sea necesaria para lograr un *"fin legítimo*", sea "*proporcionada"* para alcanzarlo y *"respetuosa"* con el contenido del derecho. Y, en el caso analizado, dada la competencia de PROSEGUR de vigilancia en el CPD del banco de Santander conceptuado como de alta seguridad el uso del teléfono y en mayor medida la aplicación whatsapp que exige el continuo tratamiento de textos durante el desarrollo del desempeño profesional puede suponer un menoscabo en las funciones de vigilancia, por lo que el fin de la restricción era legítimo para el cumplimiento del contrato, es proporcionado pues se da la alternativa de utilización de teléfonos de la empresa y respetuosa en cuanto que se informa previamente a los afectados de la restricción (prohibición).

Se cumple así el juicio de ponderación exigido por el Tribunal Constitucional en, por todas, la STC 98/2000. Era una medida justificada ya que se había preadvertido, informado y dado alternativas; idónea para la finalidad pretendida por la empresa (verificar la comisión de las irregularidades y en tal caso adoptar las medidas disciplinarias correspondientes); y equilibrada (pues la utilización de la información se limitó a constatar el uso del teléfono privado sin acceder a información adicional alguna).

Tales restricciones se dan entre otros medios de control, en 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, junto a la restricción en el uso del teléfono móvil.

La citada STS de 26/07/2009, recoge lo siguiente: "*Así, nuestra sentencia de 5 de diciembre de 2003, sobre el telemarketing telefónico, aceptó la legalidad de un control empresarial consistente en la audición y grabación aleatorias de las conversaciones telefónicas entre los trabajadores y los clientes «para corregir los defectos de técnica comercial y disponer lo necesario para ello", razonando que tal control tiene "como único objeto ...la actividad laboral del trabajador", pues el teléfono controlado se ha puesto a disposición de los trabajadores como herramienta de trabajo para que lleven a cabo sus funciones de "telemarketing" y los trabajadores conocen que ese teléfono lo tienen sólo para trabajar y conocen igualmente que puede ser intervenido por la empresa. El control de los ordenadores se justifica también por la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores (pedidos, relaciones con clientes...), por la protección del sistema informático de la empresa, que puede ser afectado negativamente por determinados usos, y por la prevención de responsabilidades que para la empresa pudieran derivar también algunas formas ilícitas de uso frente a terceros. En realidad, el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 del ET, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 del Estatuto de los Trabajadores".*

En la mayor parte de estos supuestos existen tratamientos de datos personales y, en consecuencia es necesario cumplir con 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 por ejemplo puede ser perfectamente razonable dotar de un dispositivo de geolocalización en tareas como la de seguridad ciudadana para las que resulte relevante conocer donde se encuentra el vehículo para próximas necesidades o establecer límites al empleo del teléfono particular cuando en un centro de alta seguridad suponga una disminución en el rendimiento de vigilancia o distracción en las tareas de seguridad que su naturaleza requiere, sin que suponga una violación del derecho a la intimidad en tanto se facilitan por el empresario medios alternativos para las comunicaciones necesarias, y no suponiendo que se tengan que imponer este tipo de restricción a todos los trabajadores de la empresa cuando su tipo de prestación no lo haga necesario.

También, 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 este sentido, lo expuesto más arriba en cuanto al control telefónico por el empresario siempre que el fin sea legítimo, proporcionado y respetuoso. Por otra parte, los datos que, en su caso, se obtengan y, almacenen deberán ser exactos y puestos al día y no podrán conservarse más tiempo del necesario, por lo que se recomienda a los empleadores fijar un plazo de conservación.

Y 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, del correo electrónico y de cualquier otro medio de comunicación. 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 su utilización, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación con fines privados o personales. 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 la utilización del teléfono privado en horas laborales.

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.

La reiterada STS de 26/09/2007, añade que *«…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 para la protección de los derechos humanos. ».

En síntesis, el Tribunal Supremo en la Sentencia de fecha 26/09/2007 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. Doctrina del Tribunal Supremo que es extensible al teléfono privado del trabajador siempre que se haya informado de buena fe, y previamente de la prohibición de su uso.

En el presente caso, está acreditado que PROSEGUR, a través de los dos comunicados internos trascritos de 09/01/2013 informó de buena fe y previamente a los trabajadores de la prohibición del uso de los teléfonos móviles de los vigilantes, conducta que observa las prescripciones previstas en la normativa sobre protección de datos y jurisprudencia consolidada y el hecho de que utilizase la información facilitada por el supervisor de los vigilantes –libremente divulgada por estos como se describe en el Fundamento Jurídico IV- para fundamentar los expedientes disciplinarios tiene cobertura legal en base al "interés legítimo" que dispone para corregir las conductas irregulares de los vigilantes que le pueden causar daños irreparables en su labor de custodia de un centro de alta seguridad, sin que ello suponga monitorización de los teléfonos particulares o la utilización de medios similares, por lo que no se desprende una infracción a la normativa sobre protección de datos y a la jurisprudencia citada.

VI

En relación a la incidencia de los hechos en el derecho constitucional al "secreto de las comunicaciones" regulado en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, el T.C en la sentencia nº 123/2002, que se remite a la sentencia 114/1984, recoge: *<< Ahora bien, es obvio que la protección constitucional está limitada a la existencia de una comunicación que se desea mantener secreta por sus interlocutores «la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia "erga*

omnes") ajenos a la comunicación misma. La presencia de un elemento ajeno a aquéllos entre los que media el proceso de comunicación, es indispensable para configurar el ilícito constitucional aquí perfilado» …. *Así las cosas, cabe entender razonablemente que no tiene el carácter de comunicación, desde el punto de vista constitucional, el envío de información por parte de una persona con la finalidad expresa de que su contenido sea hecho público.*

(…) La consecuencia de todo ello es que, como ordena el citado artículo 18.3 de la Constitución, el secreto de las comunicaciones se encuentra salvaguardado por la garantía jurisdiccional que determina que no puede obtenerse información sobre los datos mencionados y, por supuesto, sobre el contenido de la comunicación sin mediar autorización judicial con el riesgo manifiesto de que las pruebas que se recaben sin ella sean consideradas pruebas ilícitas. Ahora bien, esta conclusión presenta una excepción correctamente advertida en los informes de reiterada cita cuando, con apoyo en la sentencia del Tribunal Constitucional n° 56/2003, de 24 de marzo, admite ***"la posibilidad de que el secreto fuera levantado como consecuencia de la acción de uno de los dos intervinientes en la comunicación, en cuyo caso, la revelación de la información referida a la misma, incluyendo los datos identificativos de las líneas llamante y conectada, dejaba de encontrarse protegido por el mencionado secreto" >>***

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 ***PROSEGUR COMPAÑIA DE SEGURIDAD, S.A.*** 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