Expediente Nº: E/01017/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la ***ASOCIACION ANDALUZA DE LA EMPRESA FAMILIAR*** en virtud de denuncia presentada por Dª. ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 2 de diciembre de 2014, tuvo entrada en esta Agencia escrito de D.ª ***A.A.A.*** en el que denuncia que la **Asociación Andaluza de la Empresa Famliar** -AAEF- , en la que ha prestado servicios como trabajadora por cuenta ajena, instaló en el ordenador de sobremesa que utilizaba la dicente un software de auditoría denominado eBLASTER. Dicho programa, denominado coloquialmente espía, copia de forma automática la utilización del ordenador, en cuanto a programas lanzados, archivos descargados, combinación de teclas usadas, claves y demás datos personales que se puedan introducir en el ordenador por el usuario, enviando toda la información a una dirección de correo electrónica concreta quedando la misma archivada.

Aporta copia fragmentaria de un informe de auditoría informática en el que se señala:

> *<<Durante la Inspección del ordenador de sobremesa mencionado, se nos informa que la asociación instaló meses atrás en dicho equipo un software de auditoría denominado eBLASTER, que audita de forma automática la utilización del ordenador en cuanto a programas lanzados, combinación de teclas pulsadas, archivos descargados/subidos/borrados, páginas web visitadas y algunas otras opciones más para después enviar esta información empaquetada a una dirección de correo electrónico concreta en la que poder analizar posteriormente estos datos. Es un programa de tipo comercial que se adquiere mediante licencia de usuario por Internet y cuya eficacia está contrastada en el mercado.*
>
> *Según el informe del ANEXO I, que contiene información relevante del informe de actividad del software de auditoría del miércoles 12 de Marzo de 2014 (entre las 10:07:11 y las 11:07:13) podemos confirmar la siguiente Información:*
>
> *1. El puesto local en cuestión (ordenador de sobremesa) en el que está Instalado el software de auditoría eBlaster tiene como dirección de IP: ***IP.1*
>
> *2. El usuario registrado que aparece como que inició la sesión en el puesto local es "*****NOMBRE.1**".>>*

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. Solicitada información a la entidad auditora, de la información recibida se desprende:

a. Únicamente ha sido auditado un equipo en el que existen definidos un total de tres usuarios:

- ******NOMBRE.1***, usuario habitual del PC.
- Informático, conexiones esporádicas cada mes para labores de mantenimientos informáticos.
- Un usuario en desuso por haber dejado la asociación.

b. En el apartado de **Conclusión y recomendaciones de la inspección** el auditor manifiesta:

<<Para la inspección del puesto asignado la asociación se ha ayudado de un software de auditoria adquirido e instalado en los sistemas, llamado eBLASTER, que de forma automática al usuario que inicia sesión en el ordenador, le audita la utilización del mismo en cuanto a programas lanzados, combinación de teclas pulsadas, archivos descargados/subidos/borrados, páginas web visitadas y algunas otras opciones... para después enviarlo empaquetado por email y poder analizarlo. Es un programa de tipo comercial que se adquiere por licencias de usuario y que está contrastada su eficacia en el mercado.

Según el informe del ANEXO 1:

*1. El puesto local en cuestión tiene cómo IP: *****IP.1***

*2. El usuario que inició sesión en el puesto local es ***NOMBRE.1.*

*3. La unidad G: señalada en el reporte de actividad corresponde a una unidad extraíble tipo "pen drive" fijada en el equipo con IP ***IP.1.*

4. Los 286 archivos que se tratan en el reporte son previamente examinados, seleccionados y clasificados para su empaquetación de manera selectiva por el usuario para su movimiento.

5. Según muestra el informe, los 286 archivos en cuestión fueron copiados a la unidad G: extraíble (pen drive) en la fecha de **12/03/2014** *entre las 10:07:47 y las 10:16:39…*

*Una vez claro el entorno y estudiado el reporte, concluiremos después de analizar el proceder de los hechos. Es clara la utilización de un pen drive para la extracción de los 286 archivos que consta en el reporte de actividad diario emitido por el software **eBLASTER**, dicha extracción se realizó a través del PC con IP *****IP.1** y el usuario con el que se hizo log-in durante dicho periodo de tiempo era *****NOMBRE.1**.>>*

c. Consta en el Anexo 1 del informe la actividad del usuario ******NOMBRE.1***, estando habilitadas todas las doce opciones de seguimiento de actividad de que consta la aplicación, si bien solo ha habido actividad en cinco de ellas.

- Sitios web visitados. No se detalla la actividad.
- Actividad de correo electrónico. No se detalla la actividad.
- Teclas pulsadas. No se detalla la actividad.
- Actividad de programas. Se muestran los programas iniciados, la fecha y

hora de inicio, el tiempo de actividad y el número de pulsaciones de teclado.

- Seguimiento de documentos. Se muestra el nombre de los ficheros abiertos, el programa utilizado, la unidad y carpeta en que estaban ubicados, la acción realizada, así como fecha y hora en que fue realizada.

2. De la información y documentación aportada por AAEF, se desprende:

    a. Informa la entidad que la denunciante ha sido debidamente informada de las limitaciones de uso de los medios informáticos que la AAEF puso a su disposición para el correcto desempeño de sus labores profesionales. En prueba de ello aporta un correo electrónico emitido en fecha 12/5/2014, en donde se explicita:

<<3) Sobre el uso de equipos telefónicos e informáticos: los teléfonos y ordenadores de la AAEF, tanto fijos como portátiles, son herramientas de trabajo puestas a disposición de las personas que trabajan en la asociación pura ser usados exclusivamente en el desempeño de las tareas laborales encomendados, no estando en ningún momento autorizado su uso para temas personales sin aprobación previa de la dirección, siempre por causa justificada y con carácter excepcional.>>

El documento aparece firmado con un “Recibí y conforme” por la denunciante.

    b. Respecto de la acreditación de que la denunciante hubiese sido informada de la existencia de un programa de auditoría y supervisión de la actividad de los medios informáticos que le fueron asignados, manifiesta la entidad que no se cuenta con dicho documento.

Manifiesta la entidad que, en el momento de la instalación del mencionado programa de auditoria, existían indicios suficientes de una actividad ilícita por parte de la trabajadora que justificaban la instalación del mismo. El hecho de no informar a la trabajadora acerca de su instalación responde a la necesidad de comprobar de forma efectiva el uso indebido que de los medios informáticos puestos a su disposición estaba realizando la misma. Por ello, el mero hecho de informar a la trabajadora acerca de la instalación del programa citado la habría puesto sobre aviso, no habiéndose podido por tanto obtener prueba fehaciente de la mencionada actividad ilícita que, con el presunto ánimo de lucro personal o de causar un perjuicio a la AAEF, venía llevando a cabo la trabajadora.

    c. En relación directa con este tema y con fecha 9 de julio de 2015, el Juzgado de lo Social n° 2 de Jerez de la Frontera ha desestimado la demanda formulada por la trabajadora contra la AAEF por despido improcedente. En dicho procedimiento se aportaron como prueba necesaria los resultados de los análisis realizados por el programa de auditoría instalado y la sentencia resultante establece que la actuación por parte de la AAEF fue en todo momento proporcionada a la situación creada por la

conducta ilícita de la trabajadora.

Aporta la entidad copia de la sentencia, en la que consta:

- La empresa instaló un programa de auditoría ***EBlaster*** desde finales de 2013, que envía información a un servidor, controlando los ficheros, pero no el volumen que se copia. Este programa registra la dirección a la que se van los ficheros, pero no su contenido.
- La denunciante llevó a cabo el 12/3/2014 una copia sin autorización en un pen drive 286 archivos del ordenador de la empresa, conteniendo información relativa a presentaciones realizadas durante varios años a la Junta Directiva (estados financieros, presupuestos, tesorería, patrocinios y todo lo relativo a la gestión de la Asociación, incluyendo Organigrama, plan de reestructuración, propuestas a realizar a la administración), así como actas de la Junta Directiva, desglose y anotación de gastos varios, documentación bancaria, base de datos de socios (actuales y potenciales patrocinadores y contactos institucionales, así como documentación relativa a impuestos pagados, según detalle de archivos relatado en la carta de despido, que se da por reproducido.
- El día 12/5/2014 se notificó a la denunciante las normas de funcionamiento en la oficina, en la que se comunica que no está autorizado el uso personal, sin aprobación previa de dirección con causa justificada y de forma excepcional, de los equipos telefónicos e informáticos de la empresa.
- La denunciante ha utilizado de forma reiterada los medios informáticos de la empresa para uso personal dentro de su jornada de trabajo:
    - De 12 al 16 de mayo 78 accesos de uso personal.
    - De 19 a 23 de mayo 207 accesos de uso personal.
    - De 26 a 27 de mayo 56 accesos de uso personal.
- La empresa ordenó una revisión de los equipos informáticos el 24/5/2014.
- Con fecha y efectos del 4/7/2014 la demandada le comunicó a la actora mediante carta su despido disciplinario.
- La empresa ha presentado denuncia por un delito de descubrimiento de secretos, dictándose auto ordenando continuar con la tramitación de las diligencias previas.

Estima el juez:

<< cumpliendo los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad), que se cumple en el caso, al ser la investigación de archivos informáticos el medio necesario para comprobar la conducta imputada, que además se descubrió al existir problemas en la recepción de los correos electrónicos en la empresa, como se ha constatado en la testifical; si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal prepósito con igual eficacia (juicio de necesidad), no alegándose ni reparándose en qué otra medida

moderada puede adoptarse para constatar lo que se hace por esos medios informáticos; 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)>>

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora 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

En el presente caso, se denuncia la instalación en el ordenador de sobremesa adscrito a la denunciante de un software denominado eBLASTER, consistente en un programa espía, que copia de forma automática la utilización del ordenador, en cuanto a programas lanzados, archivos descargados, combinación de teclas usadas, claves y demás datos personales que se puedan introducir en el ordenador por el usuario, enviando toda la información a una dirección de correo electrónica concreta quedando la misma archivada, sin ser informada y que fue utilizada para su despido disciplinario.

La LOPD en su artículo 6, dispone lo siguiente:

"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..."

Por su parte, el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores -E.T.- en su artículo 18, establece lo siguiente:

"Solo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.

Y el artículo 20 *"Dirección y control de la actividad laboral" .*

1. El trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien este delegue.

2. En el cumplimiento de la obligación de trabajar asumida en el contrato, el

trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquel en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe.

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 y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.***

La cuestión similar a la planteada ha sido tratada por esta Agencia en las resoluciones de esta Agencia, entre otras, de 19 de febrero, 5 de octubre de 2009 y 9 de febrero de 2011, al analizar si el empresario puede examinar las herramientas informáticas a disposición del trabajador, de suerte que la respuesta se debe buscar en el equilibrio entre las facultades que le son reconocidas al empresario en el artículo 20.3 del E.T. y los derechos que le son reconocidos al trabajador en el artículo 4.2. e) del E.T. que reconoce al trabajador el derecho *" al respeto de su intimidad y a la consideración debida a su dignidad"* y a lo previsto en la Constitución Española -CE- en su artículo 18.3 que establece la garantía constitucional del *"secreto a las comunicaciones"*, en particular las telegráficas, postales y telefónicas, al remitirnos a la Sentencia de fecha 26 de septiembre de 2007 del Tribunal Supremo sobre el " *control empresarial del correo electrónico"* en los términos siguientes:

<<FUNDAMENTO DE DERECHO PRIMERO:.... La sentencia considera el despido procedente, apreciando el grave incumplimiento que se produce como consecuencia de la realización de esa actividad durante el tiempo de trabajo y en un instrumento proporcionado por la empresa, valorando, por una parte, la reducción del tiempo de trabajo y el injustificado gasto para la empresa, y, de otra, la perturbación de la disponibilidad del equipo informático en una materia tan grave como el aterrizaje y el despegue de aviones. La sentencia de contraste excluye la aplicación de las garantías del artículo 18 del Estatuto de los Trabajadores, ***porque el ordenador no es un efecto personal del trabajador, sino una "herramienta de trabajo" propiedad de la empresa.***

….Porque en el presente recurso no se trata de valorar la conducta del trabajador a efectos disciplinarios, sino de resolver un problema previo sobre el alcance y la forma del control empresarial sobre el uso por el trabajador del ordenador que se ha facilitado por la empresa como instrumento de trabajo……. Hay que insistir en que no estamos ante el enjuiciamiento de una conducta a efectos disciplinarios desde la perspectiva del alcance de la protección de un derecho fundamental, como en el caso decidido por la sentencia de 20 de abril de 2.005, sino ante un problema previo sobre la determinación de los límites del control empresarial sobre un ámbito que, aunque vinculado al trabajo, puede afectar a la intimidad del trabajador.

SEGUNDO:...La cuestión debatida se centra, por tanto, en determinar si las condiciones que el artículo 18 del Estatuto de los Trabajadores establece para el registro de la persona del trabajador, su taquilla y sus efectos personales se aplican también al control empresarial sobre el uso por parte del trabajador de los ordenadores facilitados por la empresa. Pero el problema es más amplio, porque, en realidad, lo que

*plantea el recurso, desde la perspectiva de ilicitud de la prueba obtenida vulnerando los derechos fundamentales (artículo 91.1 de la Ley de Procedimiento Laboral), es la compatibilidad de ese control empresarial con el derecho del trabajador a su intimidad personal (artículo 18.1 de la Constitución) o incluso con el derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución Española), si se tratara del control del correo electrónico. El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos establece también que toda persona tiene derecho al respeto de la vida privada y familiar y prohíbe la injerencia que no esté prevista en la ley y que no se justifique por razones de seguridad, bienestar económico, defensa del orden, prevención de las infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás. El derecho a la intimidad, según la doctrina del Tribunal Constitucional, supone "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" y ese ámbito ha de respetarse también en el marco de las relaciones laborales, en las que " es factible en ocasiones acceder a informaciones atinentes a la vida íntima y familiar del trabajador que pueden ser lesivas para el derecho a la intimidad" (SSTC 142/1993, 98/2000 y 186/2000). De ahí que determinadas formas de control de la prestación de trabajo pueden resultar incompatibles con ese derecho, porque aunque no se trata de un derecho absoluto y puede ceder, por tanto, ante "intereses constítucionalmente relevantes", para ello es preciso que las limitaciones impuestas sean necesarias para lograr un fin legítimo y sean también proporcionadas para alcanzarlo y respetuosas con el contenido esencial del derecho. En el caso del uso por el trabajador de los medios informáticos facilitados por la empresa pueden producirse conflictos que afectan a la intimidad de los trabajadores, tanto en el correo electrónico, en el que la implicación se extiende también, como ya se ha dicho, al secreto de las comunicaciones, como en la denominada "navegación" por Internet y en el acceso a determinados archivos personales del ordenador. Estos conflictos surgen porque existe una utilización personalizada y no meramente laboral o profesional del medio facilitado por la empresa. Esa utilización personalizada se produce como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador como sucede también con las conversaciones telefónicas en la empresa y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa. Pero, al mismo tiempo, hay que tener en cuenta que se trata de medios que son propiedad de la empresa y que ésta facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia del empresario, que, como precisa el artículo 20.3 del Estatuto de los Trabajadores, implica que éste "**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",** aunque ese control debe respetar "la consideración debida" a la "dignidad" del trabajador.*

TERCERO. Estas consideraciones muestran que el artículo 18 del ET no es aplicable al control por el empresario de los medios informáticos que se facilitan a los trabajadores para la ejecución de la prestación laboral. El artículo 18 del ET establece que "sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo", añadiendo que en la realización de estos registros "se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo de otro

trabajador de la empresa, siempre que ello fuera posible". El supuesto de hecho de la norma es completamente distinto del que se produce con el control de los medios informáticos en el trabajo. El artículo 18 está atribuyendo al empresario un control que excede del que deriva de su posición en el contrato de trabajo y que, por tanto, queda fuera del marco del artículo 20 del Estatuto de los Trabajadores…..Por el contrario, ***las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario "como propietario o por otro título" y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen.*** *Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18, pues incluso respecto a la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del artículo 20 del Estatuto de los Trabajadores para entrar dentro de la esfera personal del trabajador.*

De ahí que los elementos que definen las garantías y los límites del artículo 18 del Estatuto de los Trabajadores, no sean aplicables al control de los medios informáticos*….. **El empresario tiene que controlar el uso del ordenador, porque en él se cumple la prestación laboral y, por tanto, ha de comprobar sí su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales. Tiene que controlar también los contenidos y resultados de esa prestación. 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 segundo lugar, la exigencia de respetar en el control la dignidad humana del trabajador no es requisito específico de los registros del artículo 18, pues esta exigencia es general para todas las formas de control empresarial, como se advierte a partir de la propia redacción del artículo 20,3 del Estatuto de los Trabajadores…. ***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 un 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 medios aplicables, no podrá entenderse que se ha vulnerado " una expectativa razonable de intimidad.."*

La segunda precisión o matización se refiere al alcance de la protección de la intimidad, que es compatible, con el control lícito que se ha hecho referencia. Es claro que las comunicaciones electrónicas y el correo electrónico están incluidos en este ámbito con la protección adicional que deriva de la garantía constitucional del secreto de las comunicaciones. La garantía de la intimidad también se extiende a los archivos personales del trabajador que se encuentran en el ordenador… Se trata más bien de rastros o huellas de la "navegación" en Internet y no de informaciones de carácter personal que se guardan con carácter reservado. Pero hay que entender que estos archivos también entran, en principio, dentro de la protección de la intimidad, sin perjuicio de lo ya dicho sobre las advertencias de la empresa>>

Habida cuenta, lo recogido en el trascrito fallo del Tribunal Supremo que, en síntesis, prevé la posibilidad de que el empresario pueda acceder al control del ordenador, 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

En el presente caso, la entidad AAEF acredita que la denunciante fue debidamente informada de las limitaciones de uso de los medios informáticos que la AAEF puso a su disposición para el correcto desempeño de sus labores profesionales al aportar un correo electrónico emitido en fecha 12/5/2014, en donde se explicita:

<<3) Sobre el uso de equipos telefónicos e informáticos: los teléfonos y ordenadores de la AAEF, tanto fijos como portátiles, son herramientas de trabajo puestas a disposición de las personas que trabajan en la asociación pura ser usados exclusivamente en el desempeño de las tareas laborales encomendados, no estando en ningún momento autorizado su uso para temas personales sin aprobación previa de la dirección, siempre por causa justificada y con carácter excepcional.>>, apareciendo el documento firmado con un "Recibí y conforme" por la denunciante.

Por lo que cabe concluir que la denunciante sí conocía las prescripciones de la AAEF sobre la utilización de las herramientas informáticas que el empresario pone a su disposición.

Respecto de la acreditación de que la denunciante hubiese sido informada de la existencia e instalación en su terminal de un programa de auditoría y supervisión de la actividad denominado eBLASTE, la entidad manifiesta que no se cuenta con dicho documento y alega que en el momento de la instalación del mencionado programa de auditoria, existían indicios suficientes de una actividad ilícita por parte de la trabajadora que justificaban la instalación del mismo y el hecho de no informar a la trabajadora acerca de su instalación responde a la necesidad de comprobar de forma efectiva el uso

indebido que de los medios informáticos puestos a su disposición estaba realizando la misma ya que el hecho de informar a la trabajadora acerca de la instalación del programa citado la habría puesto sobre aviso, no habiéndose podido por tanto obtener prueba fehaciente de la mencionada actividad ilícita que, con el presunto ánimo de lucro personal o de causar un perjuicio a la AAEF, venía llevando a cabo la trabajadora.

El trascrito artículo 18 del E.T establece que solo se podrán realizarse registros sobre la persona del trabajador en sus taquillas y efectos particulares, cuando sean necesarios para la **protección del patrimonio empresarial** y en presencia de un representante de los trabajadores si ello fuere posible, circunstancia que se estaba produciendo dado que la denunciante estaba sustrayendo información relativa a presentaciones realizadas durante varios años a la Junta Directiva así como de las actas de la Junta Directiva, desglose y anotación de gastos varios, documentación bancaria, base de datos de socios (actuales y potenciales patrocinadores y contactos institucionales, así como documentación relativa a impuestos pagados, dicha defensa del patrimonio empresarial llevó a que el empresario recabase las pruebas de la actividad delictiva para fundamentar el ejercicio de los derechos fundamentales a la defensa y tutela judicial efectiva, en el procedimiento de despido a la denunciante.

Independientemente de lo expuesto, no deja lugar a dudas la Sentencia de 9/07/2015 del Juzgado de lo Social n º 2 de Jerez de la Frontera contra el procedimiento de despido instado por la denunciante contra AAEF que, aparte de confirmar el mismo, declara conforme a derecho y "proporcional" la instalación del software de auditoria eBLASTE en base a los motivos que se recogen en el Fundamento de Derecho Segundo ,c) in fine, que no se reproducen a efectos de brevedad.

Por otra parte, presentada denuncia por AAEF por un delito de descubrimiento de secretos, el Juez declara en Auto la continuación de las diligencias previas en base: << *cumpliendo los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto* ***(juicio de idoneidad)****, que se cumple en el caso, al ser la investigación de archivos informáticos el medio necesario para comprobar la conducta imputada, que además se descubrió al existir problemas en la recepción de los correos electrónicos en la empresa, como se ha constatado en la testifical; si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal prepósito con igual eficacia* ***(juicio de necesidad)****, no alegándose ni reparándose en qué otra medida moderada puede adoptarse para constatar lo que se hace por esos medios informáticos; 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)>>*

Por todo ello procede el Archivo de las actuaciones.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a la ***ASOCIACION ANDALUZA DE LA***

EMPRESA FAMILIAR y a Dª ***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 la Directora 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.

Mar España Martí
Directora de la Agencia Española de Protección de Datos