Expediente Nº: E/03490/2009

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS** ante entidad **FONT- SALEM S.L.** en virtud de denuncia presentada ante la misma por **D. A.A.A.** y en base a los siguientes

HECHOS

PRIMERO: Con fecha **27 de octubre de 2009**, tuvo entrada en esta Agencia escrito de **D. A.A.A.** (en lo sucesivo el denunciante)en el que denuncia a la empresa **FONT-SALEM SL** (en adelante **FONT-SALEM**) por llevar a cabo de modo subrepticio una auditoria informática en el ordenador que la empresa le había asignado, lo que sirvió de justificación para su despido disciplinario por uso abusivo de Internet, con las siguientes irregularidades : no había ningún tipo de prohibición en el uso privativo de Internet, no se había avisado ni solicitado permiso al comité de empresa ni a él y se rastrearon las páginas web accedidas por él sin su conocimiento ni consentimiento.

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.- El denunciante aporta copia de la carta de despido, de 13 de marzo de 2009, que le fue remitida por la empresa, en la que se detalla el número de accesos que determina como no autorizados, indicando el propio documento qué páginas de Internet fueron accedidas de forma no autorizada y el tema o el tipo de contenido de dichas páginas. Además, en el comunicado se indica incluso la existencia de intentos de acceso a otras páginas web que el servidor bloquea, de contenido para adultos o juegos y diversión.

La carta adjunta un informe automatizado de la auditoria, que consta de 66 páginas, donde se muestra un estudio de las páginas visitadas y su categorización (motores de búsqueda, música, juegos, financiero, salud y medicina, redes sociales, etc …) así como un listado de las direcciones visitadas y la fecha y hora del acceso.

2.- Se ha solicitado información y documentación a FONT-SALEM, en concreto :

a. Alcance y ámbito de la auditoría informática que se llevó a cabo entre enero y febrero de 2009 (personal de la empresa investigado, chequeos que fueron efectuados, personal que ha tenido acceso a los datos arrojados por la auditoria, etc),

b. Información sobre la auditoria que fue facilitada a los empleados y a los representantes sindicales. Fecha en que fue facilitada dicha información. Documentación que lo acredite,

c. Información facilitada a los empleados sobre la utilización de los medios de trabajo (ordenador, correo electrónico, Internet) para fines particulares,

Ante lo cual se ha recibido la siguiente contestación:

"1. Información y ámbito de la auditoría informática que se llevó a cabo entre enero y febrero de 2009 (personal de la empresa investigado, chequeos que fueron efectuados, personal que ha tenido acceso a los datos arrojados por la auditoría etc) "

*Para garantizar la correcta actividad de FONT-SALEM**, los responsables de informática, dentro de sus funciones y de forma recurrente, verifican y auditan que no exista ninguna anomalía que ponga en riesgo los sistemas** de la compañía o se incumplan las políticas de Sistemas de Información de FONT-SALEM. En particular, tal y como se hace constar en la carta de despido de fecha 11 de marzo de 2009, **durante los meses de enero y febrero de 2009**, FONT-SALEM llevó a cabo una verificación y auditoría informática que, por un lado, tenía como objeto revisar la seguridad de los sistemas y, por otro, detectar posibles anomalías en la utilización de los medios que pone a disposición de los empleados, todo ello destinado a asignar y optimizar de un modo más eficiente el uso de los recursos informáticos por parte de los empleados de FONT-SALEM.*

*En relación con lo anterior, en aras a la mayor claridad posible sobre la información y ámbito de la auditoría informática, nos remitimos a los hechos que el juez considera probados en la Sentencia 347/2009 (hecho probado nº 6), declarando que "La empresa realizó en los meses de enero y febrero procedimiento de auditoría interna en las redes de la información con el objeto de revisar la seguridad del sistema y detectar posibles anomalías en la utilización de los medios puestos a disposición de los empleados, cuyo informe fue entregado a la administración de personal de la empresa el día 10 de marzo. En concreto, y por lo que se refiere al ordenador utilizado por los Jefes de Turno en cuyo historial de acceso a Internet aparece una gran cantidad de entradas, **se entregó a la administración de personal auditoría detallada del historial de accesos a Internet, que es el mismo que se adjuntó a la carta de despido entregada al trabajador** ".*

"2. Información sobre la auditoría que fue facilitada a los empleados y a los representantes sindicales. Fecha en que fue facilitada dicha información. Documentación que lo acredite. "

En relación a la documentación e información solicitada en el apartado 2 de la solicitud de información de la AEPD de fecha 2 de diciembre de 2009, interesa a esta parte destacar lo siguiente:

(i) En el momento en que los trabajadores se incorporan a la plantilla de FONT-SALEM se les informa y hace entrega del documento "Manual de Acogida", de lectura obligatoria y que, entre otras informaciones, contiene las Normas Internas relativas a los Sistemas de Información (apartado 5.3.2) que describen las facultades de control y auditoría sobre los Sistemas de Información que FONT-SALEM se reserva (vid apartado Cuarto posterior). Dicha documentación se encuentra asimismo colgada en la intranet de la compañía.

(ii) En la carta de despido (adjuntada como Documento nº 3) FONT SALEM procedió a informar sobre la auditoría realizada a Don A.A.A., con copia al delegado sindical y al comité de empresa de la compañía. En relación con lo anterior, destacar que, tal y como se recoge en la Sentencia del Tribunal Supremo de 26 de septiembre de 2007, dictada en un Recurso para la Unificación de Doctrina, el artículo 20.3 del Estatuto de los Trabajadores habilita al empleador para controlar los medios de comunicación electrónicos que en cada caso asigne a sus empleados para el desarrollo de sus

funciones. En este sentido, la propia Sentencia 347/2009 de constante referencia establece respecto al tema que nos ocupa que "Ninguna violación de derechos fundamentales se ha producido, entonces, por parte del empresario en el control del cumplimiento por el trabajador de sus obligaciones laborales que le atribuye el art. 20.3 del Estatuto de los Trabajadores, lo que determina que, en este punto, el motivo de impugnación del despido formulado por el actor no merezca favorable acogida. Siendo irrelevante, por otro lado, con base en los mismos argumentos, el que la empresa no informara previamente al trabajador que se iba a efectuar procedimiento de auditoría interna en las redes de la información, pues además de que, como ya se ha dicho, tal procedimiento se efectuó a nivel general de todos los equipos informáticos de la empresa y con el objeto, no solo de detectar posibles anomalías en la utilización de los medios puestos a disposición de los empleados, sino también de revisar la seguridad del sistema, la doctrina jurisdiccional (STS de 26 de septiembre de 2007 citada) ha sentado el criterio de que en supuestos como el presente no resulta aplicable el art. 18 ET".

CUARTO. Apartado 3 de la solicitud de información de la AEPD

"3. Información facilitada a los empleados sobre la utilización de los medios de trabajo (ordenador, correo electrónico, Internet) para fines particulares".

Tal y como se ha comentado en el apartado Tercero anterior, FONT-SALEM facilita a todos sus empleados el documento "Manual de Acogida" en el que, entre otras informaciones, se facilitan las normas de Seguridad de los Sistemas de Información de las Empresas del Grupo Damm (apartado 5.3.2), que transcribimos a continuación:

"5.3.2 Seguridad de los Sistemas de Información de las Empresas del Grupo Damm

Los Sistemas de Información de la Empresa sólo deberán utilizarse para llevar a cabo tareas de negocio autorizadas por la Dirección. Su uso podrá ser auditable en cualquier momento.

El uso de los Sistemas de Información de la Empresa deberá atenerse siempre a unas normas éticas básicas. Estará prohibida su utilización para el tratamiento y distribución de material ofensivo o no apropiado.

Toda la información creada, almacenada o transmitida utilizando los Sistemas de Información de la Empresa es propiedad de la misma.

La Empresa podrá acceder a información almacenada o transmitida empleando sistemas de su propiedad y se reserva el derecho de vigilar sus sistemas con propósito de auditoría, para asegurar el uso adecuado y detectar violaciones de seguridad.

Los usuarios no deben suponer que las comunicaciones que realicen empleando los sistemas de ¡a Compañía son privadas.

El DSI o el responsable de informática de cada una de las Empresas del Grupo Datnm serán los únicos encargados de la instalación del software en ¡os equipos del Grupo Damm. Debe recordar que, aunque se disponga de una licencia de uso válida para un determinado programa, es necesario que se encuentre en la lista de programas autorizados a ser instalados en un PC o estación de trabajo.

Para conectarse a los Sistemas de Información de las Empresas del Grupo Damm:

No suplante a otra persona. Utilice únicamente sus identificativos de usuario.

No conecte ningún dispositivo a los equipos de informática o de telecomunicaciones sin permiso del DSI o del responsable de informática de su Empresa.

La conexión no autorizada de sistemas v redes de las Empresas del Grupo Damm con los de entidades externas puede suponer la aparición de riesgos de seguridad de la información grave para dichas Empresas. Por esta razón este tipo de conexiones está prohibido si no existe la aprobación expresa del DSI o del responsable de informática de su Empresa. Este aspecto será controlado de forma estricta.

Si necesita acceder a Sistemas o Información externos a las Empresas del Grupo Damm, debe usar los recursos informáticos corporativos aprobados e instalados por el DSI o por el responsable de informática de su Empresa.

Los Sistemas de Información de Damm disponen de mecanismos de detección y eliminación de virus informáticos, si sospecha la presencia de un virus o el software antivirus le avisa de la existencia de un virus en un fichero el procedimiento a seguir es:

Salir del programa o documento que se esté utilizando cuanto antes, no intentando guardar los cambios en el documento. No intentar eliminarlo sino contactar inmediatamente con el DSI o el responsable de informática de su Empresa. No apagar el ordenador, pero tampoco seguir usándolo.

Si se recibe un mensaje advirtiendo de la peligrosidad de abrir un correo electrónico solicitando que se envíe el mensaje a todos los usuarios que se conozca, probablemente se trate de un falso virus. Ante un mensaje de este tipo, se debe avisar al DSI o al responsable de informática de su Empresa.

Se deben recordar los siguientes aspectos al conectarse con las Empresas del Grupo Damm u otras:

Internet es utilizado por millones de personas en todo el mundo. No todos los usuarios tienen intereses legítimos.

Se debe presumir que cualquier información no protegida (mediante cifrado, por ejemplo) que se envíe por Internet puede ser leída por personas a las que no iba dirigida.

No utilice modems ni otros sistemas de acceso a redes de datos o a Internet. En caso de necesidad, solicítelo al DSI.

El correo electrónico sólo deberá utilizarse para llevar a cabo tareas de negocio autorizadas por la Dirección. *Utilice siempre las herramientas de correo electrónico homologadas por Damm. No utilice funciones de respuesta automática de correo para responderá los mensajes recibidos por Internet, ni envíe o reenvíe cartas encadenadas. Tampoco envíe correos masivos sin previa autorización DSI o CSU. "*

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 artículo 6 de la LOPD, referido al consentimiento en materia de protección de datos, establece en su punto 1º, la necesidad de la existencia de un consentimiento, por parte del titular del dato, para el tratamiento de sus datos personales por terceros. Así, dicho artículo es del tenor siguiente:

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

Sin embargo, dicha capacidad de control sobre el tratamiento de datos por parte del titular de los mismos, no es absoluta, como determina el punto 2º del mismo artículo 6, que es del tenor 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; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado."(el subrayado es de la Agencia Española de Protección de Datos)

De acuerdo a lo anterior, en el seno de una relación laboral, existe una suerte de habilitación legal para el tratamiento de datos de los sujetos de dicha relación, dentro de los términos de la misma. A esto ha de unirse lo previsto en el artículo 20.3 del **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, que, referido a la facultad de Dirección y Control de la Actividad Laboral por parte del empresario, nos dice:**

"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."

Lo anterior confiere al empresario la capacidad para el control de la actividad de los empleados, pero ha de tenerse en cuenta que dicha circunstancia no implica la posibilidad de un tratamiento indiscriminado de los datos de los empleados, sin necesidad de consentimiento, sino que dicha posibilidad habría de acotarla dentro de los márgenes que la normativa y jurisprudencia entienda como legítimos, en orden del pacífico desarrollo de la relación laboral que justifica el tratamiento de datos, salvaguardando en todo caso el derecho a la dignidad del trabajador.

En el presente caso, el denunciante pone de manifiesto una actuación empresarial que entiende supone una vulneración de su derecho a la protección de datos de carácter personal, al haber procedido al acceso a su ordenador de empresa, sin mediar consentimiento del afectado, ni información previa al mismo ni a los representantes de los trabajadores, accediendo a los archivos temporales de su ordenador y al resto de información residida en el mismo. En este punto hemos de estudiar la normativa que se ha venido desarrollando en torno al tratamiento de datos en el seno de una relación laboral.

III

El artículo 3.a de la LOPD define "*dato de carácter personal*" como: "*cualquier información concerniente a personas físicas identificadas o identificables.*" Por su parte, el Tribunal Constitucional, en su sentencia 292/2000, de 30 de noviembre ha establecido el carácter autónomo del derecho fundamental a la protección de datos de carácter personal, sobre el derecho a la intimidad, articulándose como un poder de control y disposición de los individuos al respecto de sus datos personales*,* lo que faculta a la persona titular de los mismos, para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, pero dentro del contexto de la relación en la que se enmarca el referido tratamiento de datos, lo cual es aplicable al tratamiento de datos dentro del ámbito de las relaciones laborales.

La Unión Europea, a través del denominado "*Grupo de Berlín*", constituido en el seno de la Conferencia Internacional sobre Protección de Datos elaboró, en Agosto de 1996, el "*Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales*", donde enmarcaba dentro del ámbito de protección de la normativa en materia de protección de datos el tratamiento de datos personales en el seno de una relación profesional. Analiza dicho informe los riesgos inherentes al control y vigilancia de los empleados a través de las modernas Tecnologías de la Información y Comunicaciones y las implicaciones de dichos controles con el ámbito de privacidad del empleado. Así, el Grupo de Berlín, desarrollo una serie de recomendaciones ante la legítima práctica de control empresarial sobre la actividad laboral de los empleados, para evitar intrusiones no justificables, en la esfera de intimidad del empleado, estableciendo que "*tanto los trabajadores como sus representantes deberán ser informados del tipo de tecnología utilizada por el empresario en relación con la vigilancia y seguimiento de su actividad laboral, debiendo abstenerse el empleador de recoger datos personales que resulten excesivos en razón de la propia naturaleza de la relación laboral*". El Grupo de Berlin ha determinado que "*el control deberá ser una respuesta proporcionada del empresario ante riesgos potenciales, teniendo en cuenta el derecho a la vida privada y otros intereses de los trabajadores*"

También es relevante en dicha materia la Recomendación(89) 2 del Consejo de Europa, en la que se establecen una serie de consideraciones en torno a las condiciones de tratamiento de los datos de los trabajadores en el ámbito de la relación laboral, estableciendo que solamente con el consentimiento del interesado o bien a partir de otras garantías previstas en el Derecho interno, podrían realizarse pruebas, análisis o procedimientos, destinados a evaluar el carácter o personalidad de una persona en el seno de dichas relaciones.

Como hemos visto, nuestro derecho interno, a través del artículo 20.3 del Estatuto de los Trabajadores, ha previsto la posibilidad de que el empresario, en aras de vigilar el desarrollo de la actividad laboral, pueda ejercer las actividades de control que les sean propias, pero, como se ha manifestado, las mismas han de sujetarse a una serie de limitaciones, que garanticen asimismo, los derecho de los trabajadores. El denunciante

manifiesta que se accedió al ordenador de la empresa sin informar al trabajador ni a los representantes sindicales. Lo anterior, junto a lo visto en torno a las recomendaciones del Grupo de Berlín, puede ponerse en relación con lo establecido en el artículo 18 del Estatuto de los Trabajadores, que nos dice:

"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. 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."

Sin embargo, el Tribunal Supremo, a través de sentencias, como la dictada el 26 de septiembre de 2007 del Tribunal Supremo ante Recurso de Casación para la unificación de doctrina (966/2006) ha establecido una serie de consideraciones al respecto de los temas planteados, que han de ser tenidas en cuenta en el presente caso. Así, partimos de la capacidad del empresario para la vigilancia y control de la actividad laboral del artículo 20 del Estatuto de los Trabajadores, y el requisito establecido por el artículo 18 del mismo cuerpo legal, de información y presencia de los representantes de los trabajadores en las actuaciones de control de sus efectos particulares en el centro de trabajo. La sentencia aludida, a este respecto nos dice:

"*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 [RCL 1978, 2836]) 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 (RCL 1999, 1190, 1572) establece también que toda persona tiene derecho al respeto de la vida privada y familiar y prohibe 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. (…) 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."

"(…)Tanto la persona del trabajador, como sus efectos personales y la taquilla forman parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución del contrato de trabajo al que se extienden los poderes 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"

(…) el hecho de que el trabajador no esté presente en el control no es en sí mismo un elemento que pueda considerarse contrario a su dignidad" (el subrayado es de la Agencia Española de Protección de Datos)

Por tanto, los soportes informáticos facilitados por el empresario a los trabajadores se erigen como bienes de empresa sobre los que el empresario puede ejercer su actividad de control, que ha de ser diferenciado de los efectos personales de los trabajadores y, por tanto, sobre los que no se les aplican los requisitos que establece el artículo 18 del Estatuto de los Trabajadores. La sentencia aludida refuerza la capacidad de vigilancia sobre los soportes informáticos, al establecer:

" El empresario tiene que controlar el uso del ordenador, porque en él se cumple la prestación laboral y, por tanto, ha de comprobar si 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 (RJ 2004, 313) , 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»"(el subrayado es de la Agencia Española de Protección de Datos).

En iguales términos se manifestó la Sentencia del Juzgado de lo Social nº 5 de Valencia (347/2009) en torno a la demanda presentada por el denunciante contra FONT SALEM, que concluyó con la no existencia de actividad infractora por parte de FONT SALEM en la falta de participación del denunciante y de los representantes sindicales en la actividad de auditoria realizada por la entidad.

IV

Pese a todo lo anterior, tanto la jurisprudencia del Tribunal Supremo como el gabinete jurídico de esta Agencia de Protección de Datos, a través del informe jurídico 0247/2008, siguiendo las recomendaciones antes vistas, que a nivel europeo realizó el Grupo de Berlín, reconocen la necesidad de una actividad informativa por parte del empresario de la posible actuación intrusiva de comprobación del empleo de las herramientas informáticas facilitadas a los trabajadores. Así la referida sentencia de 26 de septiembre de 2007, a este respecto nos

dice:

"*En este punto 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 (TEDH 1997, 37) (caso Halford) y 3 de abril de 2007 (TEDH 2007, 23) (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos (RCL 1999, 1190, 1572) ."*(el subrayado es de la Agencia Española de Protección de Datos)

El informe 0247/2008 establece que "*incumbe a la empresa decidir si autoriza a su personal a navegar con dichos fines y, en caso afirmativo, en qué medida se tolera esta utilización privada*."

En el presente caso, la operativa de contratación de FONT SALEM implica facilitar a los trabajadores un Manual de Acogida que recoge las previsiones en torno al uso de los soportes informáticos, así como la posibilidad de realización de auditorias a tales efectos. Por tanto, FONT SALEM no sólo se encontraba legitimada, de acuerdo a la jurisprudencia vista y a lo determinado por el artículo 20.3 del Estatuto de los Trabajadores, a realizar actuaciones de control sobre los ordenadores proporcionados a los trabajadores, que no olvidemos que se instauran como una herramienta de trabajo, y no como un efecto personal del profesional, sino que realizó las oportunas previsiones en cuanto al uso de los mismos, que si bien, como se ha visto, se ven sometidas a un margen de actuación privada reconocido como hábito social, también encuentran limitado su alcance de acuerdo tanto al Manual de Acogida referenciado, como por lo considerado tanto jurisprudencial como doctrinalmente. Por lo anterior, hemos de determinar que la intervención en el ordenador facilitado por la empresa al afectado, no supone como tal, una actividad infractora de la normativa en materia de protección de datos, ni afectación de la intimidad del afectado, como se ha reconocido, en lo que afecta a éste punto, tanto en el proceso seguido ante el Juzgado de lo Social nº 5 de Valencia, como por las previsiones jurisprudenciales existentes.

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 **FONT- SALEM S L** y a **D. 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.

Madrid, 3 de febrero de 2010

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte