Cribado de correo electrónico. Informe Jurídico 0391/2007

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta planteada por XXX, cúmpleme informarle lo siguiente:

La consulta plantea, si la actividad de cribado de correos electrónicos desarrollada, por una empresa en Estados Unidos constituye un tratamiento de datos conforme a la Ley Orgánica 15/1999, de 13 de enero de Protección de Datos de Carácter Personal, y si además constituye una transferencia internacional de datos.

En primer lugar es preciso señalar que las direcciones de correo electrónico tienen la consideración de datos de carácter personal, así se ha señalado en el informe de fecha de 4 de junio de 2004, en el que se establecía que

> *"Ante todo, para resolver la cuestión planteada, debe partirse de la consideración de si la dirección de correo electrónico tiene el carácter de dato de carácter personal, dado que sólo en ese caso será aplicable al caso lo dispuesto en la Ley 15/1999, a tenor de lo establecido en su artículo 2.1*
>
> *La dirección de correo electrónico se forma por un conjunto de signos o palabras libremente elegidos generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona. Esta combinación podrá tener significado en sí misma o carecer del mismo, pudiendo incluso, en principio, coincidir con el nombre de otra persona distinta de la del titular.*
>
> *Un supuesto habitual en el diseño de direcciones de correo electrónico es aquél en que, voluntaria o involuntariamente, la dirección contiene información acerca de su titular, pudiendo esta información referirse tanto a su nombre y apellidos como a la empresa en que trabaja o su país de residencia (aparezcan o no estos en la denominación del dominio utilizado). En este supuesto, a nuestro juicio, no existe duda de que la dirección de correo electrónico identifica, incluso de forma directa al titular de la cuenta, por lo que en todo caso dicha dirección ha de ser considerada como dato de carácter personal.*
>
> *Ejemplos característicos de este supuesto son aquéllos en que se hace constar como dirección de correo electrónico el nombre y, en su caso, los apellidos del titular (o sus iniciales), correspondiéndose*

el dominio de primer nivel con el propio del estado en que se lleva a cabo la actividad y el dominio de segundo nivel con la empresa en que se prestan los servicios (pudiendo incluso delimitarse el centro de trabajo en que se realiza la prestación).

A la vista de lo anteriormente indicado, y dado que en la consulta se plantea la recogida indiscriminada de direcciones de correo electrónico, debe considerarse aplicable al caso lo dispuesto en la Ley Orgánica 15/1999."

Una vez delimitado que las direcciones de correo electrónico son datos de carácter personal, la actividad de cribado de correos electrónicos, desarrollada por parte de la empresa ubicada en Estados Unidos constituye un tratamiento de datos de carácter personal atendiendo al concepto de tratamiento mencionado en el artículo 3 apartado c) de la Ley Orgánica que lo define como las "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

Si bien, según se desprende de la consulta, la prestación de servicios efectuada por la Empresa americana, se limitará al cribado de los correos electrónicos por cuenta de la empresa ubicada en España, lo que le confiere a la entidad americana la consideración de encargado del tratamiento desde el punto de vista de protección de datos, definido por el artículo 3 g) de la Ley como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento", siempre que el tratamiento se límite únicamente a la actividad de cribado de correos electrónicos objeto del contrato.

Una vez delimitado que la entidad americana tienen la consideración de encargado del tratamiento, es necesario señalar que para que la consultante, responsable del tratamiento encargue a un tercero dicho tratamiento, es imprescindible que entre amabas partes se celebre un contrato que recoja lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

En lo que atañe a los requisitos formales, el artículo 12.2 impone que "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará

con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".

- Por lo que respecta al periodo de conservación de los datos, el artículo 12.3 establece que "una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

- En lo referente a la cesión de los datos, de lo establecido en el artículo 12.2 se desprende que no procederá esa cesión, de forma que los datos habrán de ser entregados única y exclusivamente al responsable del fichero. La Agencia Española de Protección de Datos ha considerado que será posible la subcontratación de estos servicios siempre y cuando se especifiquen los siguientes requisitos acumulativos, que deberán figurar en el contrato:

o a) Que los servicios a subcontratar se hayan previsto expresamente en la oferta o en el contrato celebrado entre el responsable del fichero y el encargado del tratamiento.

o b) Que el contenido concreto del servicio subcontratado y la empresa subcontratista conste en la oferta o en el contrato.

o c) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

- En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica.

- Por último, según el artículo 12.4, "en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente", siendo, en consecuencia, de aplicación el régimen sancionador establecido en los artículos 43 y siguientes de la Ley, sujetando el primero de ellos al encargado del tratamiento a dicho régimen."

A continuación, los problemas se centran en el flujo de datos que ha de efectuarse a Estados Unidos, dado que es Estado que no ofrece nivel adecuado de protección y aunque la entidad ubicada en Estados Unidos, tenga la consideración de encargado del tratamiento, en el momento en el que los datos salgan a dicho territorio tendría lugar una transferencia internacional.

Partiéndose de dicha premisa, la transmisión de los datos a terceros Estados que no otorguen un nivel adecuado de protección de datos implica la existencia de una transferencia internacional de datos, dado que así se dispone en la Instrucción 1/2000, de 1 de diciembre, de esta Agencia Española de Protección de Datos donde en su norma primera se prevé que "se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español. En particular, se considera como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero." Añadiendo en su párrafo segundo que "La transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia para verificar su cumplimiento".

En este sentido, debe recordarse que el artículo 33 de la Ley Orgánica 15/1999 exige, para que la transferencia a un tercer Estado que no ofrece un nivel adecuado de protección pueda ser debidamente autorizada que se hubiera observado lo dispuesto en la propia Ley, de forma que la transmisión de los datos, haciendo abstracción del hecho de que la misma suponga una transferencia internacional, habrá de respetar la Ley Orgánica del mismo modo que si la transmisión se produjera dentro del territorio español.

La Comisión Europea ha adoptado Decisiones en las que una parte del contrato sea el responsable del tratamiento, efectuándose la transferencia bien a un responsable (Decisiones 2001/497/CE, de 15 de Junio de 2001, y 2004/915/CE, de 27 de diciembre de 2004), bien a un encargado del tratamiento (Decisión 2002/16/CE, ya citada).

Centrándonos en ésta última, el hecho de que una de las partes en el contrato sea el responsable del fichero resulta esencial para comprender y aplicar las garantías establecidas en el contrato que permiten obtener la debida autorización para la trasferencia (en particular en las cláusulas 4 y 6), y que únicamente pueden ser efectivamente ofrecidas por el responsable del fichero, que establecerá los extremos del tratamiento a realizar, velará por la idoneidad del encargado del tratamiento seleccionado y responderá por el incumplimiento en que pudiera incurrir el mismo.

Por tanto, la transferencia amparada en las cláusulas contenidas en la Decisión 2002/16/CE únicamente es posible en caso de que el contrato sea celebrado entre el responsable del tratamiento (consultante) y el encargado del tratamiento ubicado en el tercer estado que no ofrezca un nivel adecuado de protección.

En consecuencia, para que pueda realizarse la transferencia internacional de datos a Estados Unidos, Estado que no ofrece un nivel adecuado de protección y en el que se realizará el tratamiento de datos por

cuenta del responsable del fichero, será necesario que en el contrato se encuentren recogidos los requisitos del artículo 12 de la Ley Orgánica 15/1999 y lo dispuesto en la Decisión 2002/16/CE, para así obtener la autorización del Director de la Agencia Española de Protección de Datos a la transferencia internacional de datos con destino a estados que no ofrezcan un nivel adecuado de protección.

En este sentido, debe recordarse el análisis efectuado por el Grupo de trabajo creado por el artículo 29 de la Directiva 95/46/CE, en el Dictamen 2/2006 sobre el Respeto de la Privacidad en relación con la prestación de servicios de cribado de correo electrónico en el que *"el Grupo de trabajo 29 anima encarecidamente a los proveedores de correo electrónico a que tengan en cuenta las siguientes recomendaciones, cuyo objetivo principal es que los destinatarios de correos electrónicos puedan controlar las comunicaciones que se dirigen ante todo a ellos:*
(a) el Grupo de trabajo 29 anima a utilizar la práctica que consiste en ofrecer a los abonados la posibilidad de descartar el análisis de sus correos electrónicos a efectos de detección de buzonfia, la de comprobar los correos considerados buzonfia para determinar si lo son en realidad y la de decidir qué «tipo» de buzonfia debe eliminarse mediante filtrado. Además, el Grupo de trabajo 29 acoge asimismo con satisfacción la práctica de algunos ESPs que posibilitan a sus abonados que vuelvan a permitir el análisis de sus correos electrónicos con el objetivo de filtrar buzonfia;
(b) el Grupo de trabajo 29 es también favorable al desarrollo de sistemas de filtrado que los usuarios finales pueden instalar o configurar en su terminal, en servidores de terceros o en el servidor del proveedor de correo electrónico y que les permiten controlar lo que desean y no desean recibir, con la finalidad añadida de reducir los costes inherentes a la descarga del correo electrónico no solicitado, según recuerda el considerando 44 de la Directiva 2002/58. El Grupo de trabajo 29 saluda asimismo los trabajos de investigación de otras herramientas para combatir la buzonfia de forma menos intrusiva para la privacidad.
Por otra parte, el Grupo de trabajo 29 recuerda a los proveedores de servicios de correo electrónico que analizan correos con el fin de detectar buzonfia la obligación, prevista en el artículo 10 de la Directiva de protección de datos, de informar a los abonados de sus prácticas en relación con la buzonfia de manera clara e inequívoca, tal como se detalla en sección IV del presente dictamen. Los proveedores de correo electrónico deben garantizar también la confidencialidad de los correos filtrados, que no deberían ser utilizados para ningún otro fin. (..) "*de conformidad con el artículo 5, apartado 1 de la Directiva sobre la privacidad y las comunicaciones electrónicas, queda prohibido a los proveedores de correo electrónico el filtrado, almacenamiento u otros tipos de intervención en las comunicaciones y los datos de tráfico asociados a ellas con el fin de detectar un contenido concreto sin el consentimiento de*

los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo, con arreglo a lo dispuesto en el artículo 15 de la Directiva sobre la privacidad y las comunicaciones electrónicas, aplicado por la legislación de los Estados miembros.".

Por tanto en el caso que nos ocupa, la empresa consultante, tiene en principio la condición de usuario y consiente y decide expresamente realizar ese filtrado. A hora bien el filtrado afecta a los empleados de la empresa, lo que exige informar a los mismos sobre dicho filtrado.

Asimismo si el filtrado se extendiese al contenido de los correos electrónicos, será preciso disponer de legitimación para ello, por parte del empresario. Dicha legitimación la encontramos con carácter general, en lo referente al tratamiento de los datos correspondientes a los trabajadores, cuando el mismo se efectúa en el ámbito de la relación laboral, debe señalarse que el artículo 6.2 de la Ley Orgánica 15/1999 exceptúa la obligación de recabar el consentimiento de los afectados en los supuestos en que "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".

Además el Estatuto de los Trabajadores aprobado por el Real Decreto Legislativo 1/1995, de 24 marzo, establece en su artículo 20. 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."

En virtud de lo expuesto podemos entender que existe legitimación para filtrar el contenido del correo electrónico de los empleados, pero siempre que se trate de una cuenta de correos proporcionada por la empresa para el desarrollo de sus funciones laborales y siempre que se haya informado previamente a los trabajadores sobre dicho filtrado y los medios que se van a utilizar.

A mayor abundamiento es necesario señalar que sobre el ámbito de intervención que dispone el empresario para poder controlar las cuentas de correo electrónico de sus trabajadores, se ha pronunciado la Agencia Española de Protección de Datos en un informe de fecha 10 de abril de 2006 en el que se recogía las recomendaciones y dictámenes de la Unión Europea en el que se señalaba:

" A su vez, también los trabajadores deben velar en pos del mencionado derecho, colaborando en el seno de la empresa, y contribuyendo con su aportación positiva a la implantación de cuantas

medidas de tipo técnico y organizativo resulten necesarias para una mejor protección de los datos personales del conjunto de los empleados.

Sin embargo, dicho derecho debe conciliarse con otros derechos e intereses legítimos del empleador, y en particular, con el derecho del empresario a administrar con eficacia la empresa, y sobre todo, con su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de determinadas acciones de los trabajadores. En este sentido, cabe apuntar que en ocasiones, estos derechos e intereses constituyen motivos legítimos que pueden justificar la adopción de medidas adecuadas destinadas a limitar el derecho a la vida privada de los trabajadores. Así por ejemplo en los supuestos en que el empleador es víctima de un delito imputable a un trabajador, que constituyen el ejemplo más claro.

III

En su Sentencia 292/2000, de 30 de noviembre, el Tribunal Constitucional ha venido a concretar el alcance del derecho fundamental a la protección de datos de carácter personal, estableciendo su carácter autónomo e independiente, deslindado del derecho a la intimidad, cuyo contenido persigue garantizar un poder de control de los individuos respecto de sus datos personales, así como sobre el uso y destino de los mismos, con el propósito de impedir su tráfico ilícito y lesivo. Pues bien, los argumentos y la fundamentación contenidos en dicha sentencia resultan plenamente aplicables a las relaciones laborales.

En el ámbito estrictamente laboral, existen diversos documentos internacionales que abordan la problemática de la protección de datos en el ámbito laboral. Entre ellos destacan la Recomendación (89) 2 del Comité de Ministros del Consejo de Europa, sobre la protección de los datos de carácter personal utilizados con fines de empleo, y las Recomendaciones de la Organización Internacional del Trabajo de 1996. A su vez, el "Grupo de Berlín", constituido en el seno de la Conferencia Internacional sobre Protección de Datos, se ha posicionado claramente sobre la protección de los datos en el contexto laboral a través de su documento "Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales", de agosto de 1996.

Dada su enorme relevancia, cabe referirse primer lugar a la Recomendación (89) 2 del Consejo de Europa. Dicha Recomendación es el documento que ha marcado de forma más importante los desarrollos posteriores en este campo. En la misma se afirma que la expresión "con fines de empleo" que utiliza se refiere a las relaciones entre trabajadores y empresarios en materia de reclutamiento de trabajadores, ejecución del contrato y gestión, incluidas las obligaciones

derivadas de la ley o de convenios colectivos, así como a la planificación y organización del trabajo, con lo que se pone de manifiesto la vocación de otorgar a los datos personales de los trabajadores un importante nivel de protección.

Dicha Recomendación, contiene una serie de consideraciones generales sobre las condiciones de un tratamiento leal y legítimo de los datos de los trabajadores, así como referencias específicas y concretas a diversos tipos de problemas que pueden surgir con la protección de dichos datos en el ámbito de laboral.

La Recomendación establece que sólamente con el consentimiento del interesado, o con otras garantías previstas en el Derecho interno, se podrían realizar pruebas, análisis o procedimientos destinados a evaluar el carácter o la personalidad de una persona, y también afirma el derecho del afectado a conocer el resultado de dichas evaluaciones si así lo desea.

De otra parte, en el seno del Grupo de Berlín, se ha abordado la problemática derivada del uso de las nuevas tecnologías de la información y las telecomunicaciones dentro del lugar de trabajo caracterizada, al menos potencialmente, por la indudable generación de información acerca de los trabajadores.

En su documento "Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales", el Grupo analiza los riesgos inherentes al control y vigilancia de los empleados a través de las modernas Tecnologías de la Información y de las Comunicaciones, que suponen en muchas ocasiones una intrusión en su privacidad.

La protección de los datos personales de los trabajadores tanto "en el lugar de trabajo", como en su propio domicilio, a consecuencia de la extensión del denominado "Teletrabajo", justificaron que el Grupo se definiera mediante el dictado de una serie de Recomendaciones, dirigidas a establecer los requisitos y condiciones necesarios que deberían ser respetados en la recogida de datos a través de los dispositivos propios de las nuevas tecnologías.

En dicho documento se "informa" sobre los métodos de recogida de datos más comunes utilizados en el seno de las organizaciones empresariales, tales como los dispositivos magnetofónicos, audio-visuales, transmisores de infrarrojos, identificadores de datos biométricos, dispositivos de videovigilancia, y comunicaciones electrónicas, alertando sobre los riesgos y perjuicios que el uso desviado de dichos medios puede ocasionar al trabajador.

A modo de Recomendación, y en orden a garantizar que tal uso será legítimo, necesario, adecuado, pertinente, y proporcionado a la finalidad que lo justifica, se establecen los necesarios controles, en los que se implica muy especialmente a los ***"representantes de los trabajadores"****.*

Así, 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.

A su vez, los representantes de los trabajadores obtendrán cumplida información sobre la introducción de cualquier nuevo sistema de registro de datos que afecte al conjunto de los trabajadores, teniendo estos últimos la posibilidad de acceder a los datos que se procesen sobre ellos y el derecho a rectificar los posibles errores que les afecten.

Salvo excepciones extremas, fundamentadas en una firme sospecha sobre la existencia de actividades delictivas o dolosas del trabajador, el derecho de Información en la recogida de datos constituye un requisito indispensable para utilizar, en su caso, la información recabada en el lugar de trabajo contra el propio trabajador. En este supuesto, el empleado deberá tener la oportunidad de acceder a la información que le es adversa a fin de poder rebatirla.

Finalmente, se intenta preservar un espacio "libre de vigilancia", donde la intimidad del trabajador quede garantizada a salvo de cualquier intromisión del empresario. Dicha "zona franca" se fundamenta en el respeto de la "dignidad humana", y despliega su contenido esencial en el ámbito de la comunicación libre con el resto de los trabajadores de la empresa.

Finalmente, en el ámbito de la Unión Europea, destacan tres importantes Documentos de Trabajo del "Grupo del Artículo 29", constituido al amparo de la Directiva sobre Protección de Datos, a saber:

El Dictamen 8/2001, sobre el tratamiento de datos personales en el contexto laboral (13-9-2001), adoptado por el Grupo de Trabajo del Artículo 29, insiste en la idea de que tanto los estados de la Unión, como los diferentes agentes sociales, deben tomar conciencia de que muchas de las actividades realizadas de forma rutinaria en el ámbito de la empresa implican el tratamiento de datos personales de los trabajadores y, en muchas ocasiones, de información de carácter personal especialmente protegida.

La recopilación, almacenamiento y uso de información sobre los trabajadores por medios electrónicos, y las diversas herramientas de uso común en buena parte de las empresas, tales como el correo electrónico o el acceso a Internet, implican en muchas ocasiones el tratamiento de datos personales de los trabajadores. A ello se unen otras nuevas modalidades de control del trabajador, que llegan de la mano de la imagen y el sonido, entre las que destacan los sistemas de videovigilancia a los que se debe aplicar la normativa sobre protección de datos.

En este Dictamen, el Grupo enumera y desarrolla los Principios Fundamentales de la Protección de Datos, que los empresarios deberán tener siempre en cuenta en el contexto laboral. Así, los principios de Finalidad y de Transparencia, referidos a la necesidad del uso legítimo de los datos, adecuados a un fin determinado y explícito, propio de la actividad laboral, y a la necesidad de que los trabajadores conozcan qué datos recoge el empresario sobre ellos. Según se apunta en el Dictamen, la Transparencia también podría garantizarse otorgando al interesado el derecho de acceso a los datos personales que les afectan. De este modo, los trabajadores, como partes interesadas en la relación laboral, deben beneficiarse de los derechos que confiere la Directiva sobre protección de datos y, muy especialmente, del derecho de acceso, previsto en el artículo 12 de la misma.

El principio de legitimidad se vincula al de proporcionalidad, debiendo ser los datos recabados, adecuados, pertinentes y no excesivos en relación con la necesidad de su recogida, y disponiéndose la necesidad de que los trabajadores sean suficientemente informados sobre la existencia de dicho tratamiento legítimo y proporcionado. Así, en lo referente a vigilancia de los trabajadores a través del correo electrónico, Internet, cámaras de vídeo o datos de localización, 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.

*A su vez, es responsabilidad inexcusable del empresario, velar por la exactitud, actualización y conservación de los datos, adoptando las medidas de seguridad necesarias que preserven la información obtenida al ámbito propio de la empresa, impidiendo el acceso indebido o la difusión no autorizada de dichos datos. También el empresario deberá ofrecer una correcta "Formación al Personal" **encargado del tratamiento de los datos** en el seno de la empresa, a fin de garantizar adecuadamente la protección de los datos de los trabajadores.*

Especial mención merecen dos importantes cuestiones abordadas por el Dictamen al que se refiere el presente análisis, como son el tratamiento del "Consentimiento" del trabajador en el contexto laboral, y la "Interacción entre la legislación laboral y la legislación sobre protección de datos".

Por lo que respecta al "Consentimiento", el Grupo del artículo 29 considera que si un empresario debe tratar datos personales como consecuencia inevitable y necesaria de la relación laboral, no debería legitimar este tratamiento a través del consentimiento. Por el contrario, el recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello.

Finalmente, el "Grupo de trabajo" apunta que la legislación sobre protección de datos no debe aplicarse de forma independiente del Derecho del Trabajo y las prácticas laborales y que éstos, a su vez, no pueden aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos. Esta interacción es necesaria y valiosa y debería contribuir al desarrollo de soluciones que protejan adecuadamente los intereses de los trabajadores.

De otra parte, la Recomendación 1/2001, sobre datos de evaluación de los trabajadores (22-3-2001), adoptada por el Grupo del Artículo 29 comienza delimitando, muy brevemente, y de acuerdo con la definición contenida en la Directiva sobre Protección de Datos, lo que debe entenderse por datos personales.

En consideración al alcance de dicha definición, que engloba a "todo tipo de información sobre una persona física identificada o identificable, tal como los datos relacionados con su identidad física, fisiológica, psíquica, económica, cultural o social", se concluye que se pueden encontrar datos personales en las evaluaciones y juicios subjetivos que incluyen este tipo de elementos.

En conclusión, se aboga a favor de que los datos subjetivos, procedentes de evaluaciones o juicios subjetivos realizados sobre los trabajadores, sean siempre accesibles a los mismos y admitan su rectificación. Para ello resulta indispensable la transparencia en el tratamiento de este tipo de datos, y el respeto del ejercicio del derecho de acceso.

IV

Finalmente, el Documento de Trabajo del "Grupo del Artículo 29", relativo a la vigilancia de las comunicaciones electrónicas en lugar de

trabajo (29-5-2002), examina la vigilancia por el empleador de la utilización del correo electrónico e Internet por parte de los trabajadores, ofreciendo una orientación y ejemplos concretos sobre lo que constituyen actividades de control legítimas y límites aceptables de la vigilancia de los trabajadores por el empresario. Es preciso señalar que el documento de trabajo cubre toda actividad vinculada a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, tanto la vigilancia en tiempo real como el acceso a datos almacenados.

Para equilibrar el derecho a la vida privada de los trabajadores y el poder de dirección del empresario es preciso tener en cuenta varios principios y, en particular, el principio de proporcionalidad. En este sentido, el empleador deberá tener en cuenta la necesaria ponderación en la adopción de cualquier medida de vigilancia.

En relación con el uso de Internet con fines privados en el lugar de trabajo, 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.

Toda medida de control deberá ser "proporcionada" al riesgo que corre el empresario. A su vez, el empleador debe dar prioridad al principio de Transparencia, informando correctamente a los trabajadores de las condiciones en que se autoriza la utilización de Internet con fines privados.

Respecto al uso del correo electrónico, como recomendación práctica, los empleadores podrían considerar las ventajas de proporcionar a los trabajadores dos cuentas de correo; una de uso profesional exclusivo, en la que se permitiría un control dentro de ciertos límites; y otra de uso estrictamente privado (o con autorización de utilizar el correo web), que sólo sería objeto de medidas de seguridad y que se controlaría para prevenir abusos en casos excepcionales.

El apartado 3 del Documento se refiere a los principios generales aplicables a la vigilancia de las comunicaciones electrónicas, destacando los de "Necesidad", "Finalidad", "Transparencia", "Legitimidad", "Proporcionalidad", "Exactitud y Conservación de los Datos" y "seguridad". Dichos principios se abordan desde la perspectiva de la Directiva sobre Protección de Datos Personales por lo que, en general, las conclusiones que se obtienen resultan similares a las que se extraen en relación con cualquier otro ámbito o actividad al que resulte aplicable dicha normativa.

En esta detallada regulación destaca el principio de "Transparencia", en virtud del cual se establece la obligación de

proporcionar al trabajador información sobre la política de la empresa relativa a la vigilancia del correo electrónico y la utilización de Internet, así como sobre los motivos y finalidad de la vigilancia, la información detallada sobre el tipo de medidas de vigilancia adoptadas, y los procedimientos de aplicación e infracción de las directrices internas relativas al uso de estas herramientas.

A su vez, los derechos de acceso, rectificación, y cancelación y/o bloqueo, adquiere un especial protagonismo. Así, el trabajador debe poder acceder sin restricciones y con una periodicidad razonable a los archivos del empleador referentes a las actividades de vigilancia en el lugar de trabajo que le afecten.

En general el "Grupo del Artículo 29" entiende que los mensajes electrónicos deben beneficiarse de la misma protección de los derechos fundamentales que el "correo tradicional", y opina que las comunicaciones electrónicas que proceden de locales profesionales pueden estar cubiertas por los conceptos de "vida privada" y de "correspondencia" (según lo dispuesto en el Art. 8.1 del Convenio Europeo). Así, el secreto de las comunicaciones y de la correspondencia no dependen de la ubicación y la propiedad de los medios electrónicos utilizados, según se establece en constituciones y principios jurídicos fundamentales.

A sensu contrario, la legitimación más idónea de la vigilancia del correo electrónico puede encontrarse en la letra f) del artículo 7 de la Directiva, que prevé que el tratamiento sólo pueda efectuarse si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos.

Sin embargo, cuando el trabajador recibe una cuenta de correo electrónico para uso estrictamente personal o puede acceder a una cuenta de correo web, la apertura por el empleador de los mensajes electrónicos de esta cuenta (excepto para detectar virus) sólo podrá justificarse en circunstancias muy limitadas y no podrá ampararse normalmente en la mencionada letra f) del artículo 7, ya que acceder a este tipo de datos no es necesario para satisfacer un interés legítimo del empleador. En este caso, prevalece por el contrario el derecho fundamental al secreto de la correspondencia.

En consecuencia, la cuestión de en qué medida el artículo 7.f) autoriza el control del correo electrónico ***depende de la aplicación caso por caso*** *de los principios generales sobre protección de datos, sopesando no solo los intereses de las partes, sino también el respeto*

de la vida privada de las personas ajenas a la organización afectadas por la actividad de vigilancia".

Por último, la reciente Sentencia del Tribunal Supremo de 26 de septiembre de 2007, dictada en un Recurso para la Unificación de Doctrina, viene a confirmar la obligación de informar al trabajador sobre las reglas de uso del ordenador y los controles que sobre los mismos efectuará el empresario, dentro del poder que le confiere el artículo 20.3 del Estatuto de los trabajadores, así el fundamento jurídico cuarto señala que:

"CUARTO.- El control del uso del ordenador facilitado al trabajador por el empresario no se regula por el artículo 18 del Estatuto de los Trabajadores, sino por el artículo 20.3 del Estatuto de los Trabajadores y a este precepto hay que estar con las matizaciones que a continuación han de realizarse. La primera se refiere a los límites de ese control y en esta materia el propio precepto citado remite a un ejercicio de las facultades de vigilancia y control que guarde "en su adopción y aplicación la consideración debida" a la dignidad del trabajador, lo que también remite al respeto a la intimidad en los términos a los que ya se ha hecho referencia al examinar las sentencias del Tribunal Constitucional 98 y 186/2000. 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 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos."