Informe 0247/2008

La consulta plantea, que procedimientos debe de seguirse en cuanto al uso de los correos electrónicos de los trabajadores por parte de las empresas según la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

Es preciso indicar, que las competencias de la Agencia Española de Protección de datos, se centran en la necesidad de valorar el correcto tratamiento que de los datos personales se efectúa por parte de los responsables.

En el supuesto de hecho planteado en la consulta, alude a la posibilidad de acceder a la información contenida en los correos electrónicos que el empresario pone a disposición del trabajador, para el desarrollo de su actividad laboral.

Para poder acceder a dicha información, resulta necesario que exista legitimación para dicho tratamiento de datos, y el artículo 6.1 de la citada Ley Orgánica dispone que "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga lo contrario", no obstante 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".

No obstante el Estatuto de los Trabajadores aprobado por el Real Decreto Legislativo 1/1995, de 24 marzo, establece en su artículo 20. 3 que "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, no podemos dejar de destacar la reciente Sentencia del Tribunal Supremo de 26 de septiembre de 2007, dictada en un Recurso para la Unificación de Doctrina, donde se 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."

En conclusión, podemos señalar que el artículo 20.3 del Estatuto de los Trabajadores habilita al Empresario a controlar el correo electrónico que él otorga a los trabajadores para el desarrollo de sus funciones, pero siempre que previamente haya informado sobre dicho extremo y cumpla de ese modo el deber de informar previsto en el artículo 5.1 de la Ley Orgánica 15/1999.