Informe 0417/2009

La consulta plantea diversas dudas en relación con la posible adecuación a la normativa de protección de datos de un proceso de control realizado por el Administrador de red de un Organismo Público.

Según se indica en la consulta el servidor se encuentra dividido en varias Unidades de Red adaptadas a las necesidades de trabajo, disponiendo cada usuario de una Unidad de Red de acceso exclusivo, a la que se denomina en la consulta unidad H. Por motivos de gestión de la red, el administrador ha realizado una auditoria en dicha unidad consistente en confeccionar un listado, en el que se encuentran identificados de forma individualizada cada uno de los empleados del centro junto con el nombre y extensión de cada uno de los ficheros que se encuentran en dicha unidad H y que fue entregado al director del centro.

La consulta plantea muy diversas cuestiones que en algunos aspectos exceden del ámbito del derecho fundamental a la protección de datos personales, y cuya solución se encuentra más propiamente en el ámbito del derecho laboral o del administrativo en lo relativo al desenvolvimiento de la relación funcionarial, o en la protección de otros derechos fundamentales como el derecho a la intimidad recogido en el artículo 18.1 de la Constitución y cuya tutela no corresponde a esta Agencia.

Desde la óptica del derecho a la protección de datos personales la primera cuestión que es preciso determinar es si los datos obtenidos en la forma expresada en la consulta constituyen datos de carácter personal. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal define a éstos en su artículo 3.a) como "*cualquier información concerniente a personas físicas identificadas o identificables.*"

Por su parte, el artículo 5.1 del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa que constituye un dato de carácter personal *"*Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*."*

También en lo que se refiere al concepto de datos personales, cabe mencionar la Recomendación 1/2001, sobre datos de evaluación de los trabajadores, adoptada por el Grupo del Artículo 29 órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Señala dicha Recomendación que:

"Según la definición incluida en la letra a) del artículo 2 de la Directiva 95/46/CE, los datos personales son toda información sobre una persona física identificada o identificable, tal como los datos relacionados con su identidad física, fisiológica, psíquica, económica, cultural o social.

El alcance de dicha definición implica que los datos personales incluyen, además de los datos de los registros de población o información resultante de factores objetivos que se pueden verificar o rectificar, cualquier otro elemento, información o circunstancia que incluya un contenido informativo tal que se sume al conocimiento de una persona identificada o identificable.

Así, se pueden encontrar datos personales en evaluaciones y juicios subjetivos que, en realidad, podrían incluir elementos específicos de la identidad física, fisiológica, psíquica, económica, cultural o social de los interesados. Esto sucede igualmente si un juicio o evaluación se resume en una puntuación o clasificación, o si se expresa mediante otros criterios de evaluación."

En este mismo sentido, el Dictamen 4/2007 del Grupo de trabajo del artículo 29, sobre el concepto de datos personales señala que *"un dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa".* Así para considerar *"que los datos versan sobre una persona, debe haber un elemento "contenido", o un elemento "finalidad" o un elemento "resultado". "*

Por consiguiente para determinar si en el supuesto sometido a consulta nos encontramos ante un tratamiento de datos personales habrá que acudir a cada caso en concreto para ver si se produce alguna de las circunstancias citadas por el grupo de trabajo del artículo 29, sin que del hecho de que se haya listado el nombre de los ficheros con sus correspondientes extensiones asociado al titular pueda deducirse, en principio, que se trata de datos personales, en tanto que el nombre asignado al fichero no tiene porqué corresponderse con su contenido. No obstante, tal y como señala el dictamen del Grupo de Trabajo la utilización de ese listado con la finalidad de evaluar a los empleados del Organismo podría dar lugar a su consideración como un dato personal, lo mismo ocurriría si, a pesar de la ausencia de los otros elementos, existe un elemento de resultado, esto es, si teniendo en cuenta todas las circunstancias que rodean al caso concreto la información repercute en los derechos y los intereses de una persona determinada.

Si del análisis anterior se concluye que nos encontramos ante datos de carácter personal, será de aplicación la Ley Orgánica 15/1999, entre cuyos principios debe mencionarse, en primer lugar el relativo a la necesidad de

legitimación para efectuar el tratamiento de dichos datos, así como la calidad, especialmente en sus aspectos de finalidad y proporcionalidad del tratamiento.

Con carácter previo al examen de la normativa nacional, cabe señalar que existen diferentes instrumentos internacionales que abordan la problemática del tratamiento de datos en el ámbito de las relaciones laborales.

Así el Grupo de Berlín, constituido en el seno de la Conferencia Internacional sobre Protección de Datos, en su documento "Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales", 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.

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.

Señala también, que 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.

Por su parte el Grupo de Trabajo del artículo 29 en su Dictamen 8/2001, sobre el tratamiento de datos personales en el contexto laboral, 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.

Indica este Dictamen que *"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."*

Asimismo, en el citado 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.

En nuestro derecho el artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 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, el número segundo del mismo artículo, exceptúa la obligación de recabar el consentimiento de los afectados en diversos supuestos, de los cuales interesa aquí el citado en dicho inciso al disponer que "*No será preciso el consentimiento cuando 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".

La legitimación para el tratamiento de los datos a que se refiere la consulta derivará de la existencia de la relación laboral o funcionarial, relación que se desenvolverá conforme a la normativa que le es aplicable. En el marco de la Administración Pública, es preciso tener en cuenta aquí lo previsto en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, cuyo artículo 42.2, crea el Esquema nacional de Seguridad, cuyo objeto es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Este Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica viene regulado en la actualidad por el Real Decreto 3/2010, de 8 de enero, que dispone en su artículo 1 " 1. *El presente real decreto tiene por objeto regular el Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, y determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley.*

2. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias."

Dicho Real Decreto contiene diversas referencias a la supervisión y control del personal para garantizar la seguridad de los sistemas, así el artículo 14 señala que "*Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos."* Asimismo, el artículo 23 prevé que *"Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente Real Decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa*."

El artículo 11 de dicho Real Decreto determina que “Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.”

Por consiguiente, es en el marco de dicha política de seguridad, en el que deben desenvolverse los controles sobre los medios electrónicos puestos a disposición de los empleados públicos para el ejercicio de sus funciones. Dichos controles deberán ser respetuosos, con los principios del derecho fundamental a la protección de datos personales, en particular con los principios de información, finalidad y proporcionalidad.

En lo que se refiere a la información, además de lo previsto en el artículo 14 del aludido Real Decreto debe destacarse lo declarado en la Sentencia del Tribunal Supremo de 26 de septiembre de 2007, dictada en un Recurso para la Unificación de Doctrina, referida a 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. Sentencia que, por otra parte, resuelve algunas de las cuestiones planteadas en la consulta, por lo que se reproduce a continuación su fundamento jurídico cuarto :

“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."

Resultan, también de interés a este respecto los criterios fijados por esta Agencia en su "guía de protección de datos en las relaciones laborales," en la que se indica que:

"*Debe cumplirse con el deber de información a los trabajadores. Este deber resulta particularmente relevante cuando se trate de controles sobre el uso de Internet y/o del correo electrónico.*

En este caso es muy recomendable que la información a los trabajadores sea clara en lo que respecta a la política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales. Así como que incluya la finalidad de la vigilancia, y cuando pueda repercutir sobre medios que el trabajador utiliza normalmente una información sobre las medidas de vigilancia adoptadas.

Por otra parte, en la medida en la que este tipo de controles inciden sobre el conjunto de la empresa puede ser muy recomendable informar también a los representantes de los trabajadores del as políticas adoptadas en esta materia.

No se trata en absoluto de que el trabajador conozca el detalle de políticas de seguridad que pueden afectar a ámbitos que la empresa necesita proteger. Sin embargo, es indispensable que conozca, por ejemplo, si puede recibir mensajes privados, o depositar fotografías en determinados espacios en su ordenador o en un servidor corporativo."

Por otra parte, los controles a realizar deben ajustarse a los principios de finalidad y proporcionalidad previstos en el artículo 4 de la Ley Orgánica 15/1999, según el cual **"***Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las*

*finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.***"**

La finalidad determinada, explicita y legítima vendrá dada en el presente caso por la necesidad de garantizar la seguridad de los sistemas, informáticos, de esta manera las notas técnicas sobre volumen y limitación de utilización a que hace referencia la consulta contribuyen a especificar cual es la finalidad del tratamiento de datos, debiendo analizarse si dicho tratamiento se ajusta a los requerimientos de proporcionalidad del artículo 4 de la Ley Orgánica 15/1999.

Respecto de la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de "*una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.*

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

Por consiguiente, cualquier medida de control que se adopte debe superar este juicio de proporcionalidad, determinando si la medida es adecuada, necesaria y equilibrada, ya que en otro caso resulta desproporcionada y por ello contraria a la normativa de protección de datos.

Resulta así recomendable que los controles se realicen mediante sistemas estadísticos que generen indicadores de gestión o de uso que detecten, en su caso, posibles comportamientos desviados de los usos particulares permitidos, en la política de seguridad de la empresa u organismo, de los medios electrónicos utilizados, de manera que se recojan solamente aquellos datos adecuados, pertinentes y no excesivos, en los términos del artículo 4 de la Ley Orgánica 15/1999.