Informe 0615**/**2009

La consulta plantea si resulta conforme a la normativa de protección de datos el Reglamento de utilización de bienes informáticos aprobado por el Ayuntamiento al que pertenece el comité de empresa consultante. En dicho Reglamento, se prevén las medidas de supervisión aplicables a la utilización de los sistemas de información del Ayuntamiento, haciendo referencia a aspectos como el uso del correo electrónico y acceso a Internet por los empleados, entre otras cuestiones.

I

Con carácter previo al examen de la adecuación de dicha norma a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, cabe señalar que existen diferentes instrumentos internacionales que abordan la problemática del tratamiento de datos personales 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, 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, 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 el Dictamen 8/2001 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."*

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 la 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.

Entre los instrumentos internacionales a los que se viene haciendo referencia debe mencionarse especialmente el Documento de Trabajo del Grupo del Artículo 29, relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo de 29 de mayo de 2002, en el que se 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.

Cabe destacar que dicho Documento de Trabajo señala respecto del principio de proporcionalidad que "*Según este principio, los datos personales, incluidos los que se utilicen en las actividades de control, deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben. La política de la empresa en este ámbito deberá adaptarse al tipo y grado de riesgo al que se enfrente dicha empresa.*

El principio de proporcionalidad excluye por lo tanto el control general de los mensajes electrónicos y de la utilización de Internet de todo el personal, salvo si resulta necesario para garantizar la seguridad del sistema. Si existe una solución que implique una intromisión menor en la vida privada de los trabajadores y que permita lograr el objetivo perseguido, el empleador debería considerar su aplicación (por ejemplo, debería evitar los sistemas que efectúan una vigilancia automática y continua).

Si es posible, el control del correo electrónico debería limitarse a los datos sobre tráfico de los participantes y a la hora de una comunicación más que al contenido, si ello es suficiente para satisfacer las necesidades del empleador. Si el acceso al contenido de los mensajes es indispensable, convendría tener en cuenta el respeto de la vida privada de los destinatarios externos e internos de la organización. Por ejemplo, el empleador no puede obtener el consentimiento de las personas ajenas a la organización que envían mensajes

a los miembros de su personal. Del mismo modo, el empleador debería aplicar todos los medios razonables para informar a las personas ajenas a la organización de la existencia de actividades de vigilancia que pudieran afectarlas. Se podría, por ejemplo, insertar avisos de la existencia de sistemas de vigilancia en todos los mensajes salientes de la organización.

La tecnología ofrece al empleador importantes posibilidades de evaluar la utilización del correo electrónico por sus trabajadores, comprobando, por ejemplo, el número de mensajes enviados y recibidos o el formato de los documentos adjuntos; por ello la apertura efectiva de los mensajes electrónicos es desproporcionada. La tecnología puede también utilizarse para garantizar que sean proporcionadas las medidas adoptadas por el empleador para proteger de todo abuso el acceso a Internet autorizado a su personal, utilizando mecanismos de bloqueo más que de vigilancia."

En cuanto a la utilización de Internet por los trabajadores indica dicho Documento de trabajo que *"En la medida de lo posible, **la prevención debería primar sobre la detección**. En otras palabras, al empleador le es más beneficioso prevenir la utilización abusiva de Internet por medios técnicos que destinar recursos a su detección. Dentro del límite de lo que es razonablemente posible, la política de la empresa respecto a Internet debería basarse en herramientas técnicas para limitar el acceso, más que en dispositivos de control de los comportamientos, por ejemplo, bloqueando el acceso a algunos sitios o instalando advertencias automáticas.*

*El suministro al trabajador de información rápida sobre la detección de una utilización sospechosa de Internet es importante para minimizar los problemas. Aunque sea necesaria, toda medida de control debe ser **proporcionada** al riesgo que corre el empleador. En la mayoría de los casos, la utilización abusiva de Internet puede detectarse sin tener que analizar el contenido de los sitios visitados. Por ejemplo, la comprobación del tiempo empleado o la elaboración de una lista de los sitios más visitados por un servicio podría bastar para confirmar al empleador que sus sistemas se emplean correctamente. Si estas comprobaciones generales revelaran una posible utilización abusiva de Internet, el empleador podría entonces considerar la posibilidad de proceder a nuevos controles en la zona de riesgo.*

*Al analizar la utilización de Internet por los trabajadores, los empleadores **deberían evitar sacar conclusiones precipitadas**, dada la facilidad con que pueden visitarse involuntariamente algunos sitios a través de respuestas de motores de búsqueda, vínculos hipertextuales ambiguos, pancartas publicitarias engañosas o errores al pulsar las teclas.En todos los casos, deberán presentarse al trabajador en cuestión todos los hechos de que se le acusa y ofrecerle la posibilidad de refutar la utilización abusiva alegada por el empleador."*

Menciona este documento que ya existen numerosos ejemplos prácticos de la utilización de los medios tecnológicos a que se refiere, citando los siguientes:

"- Internet: algunas empresas utilizan un programa informático que puede configurarse para impedir la conexión a categorías predeterminadas de sitios web. Tras consultar la lista global de los sitios web visitados por su personal, el empleador puede decidir añadir algunos sitios a la lista de los bloqueados (eventualmente después de haber informado a los trabajadores de que se bloqueará la conexión con este sitio, salvo si un trabajador le demuestra la necesidad de conectarse).

- Correo electrónico: otras empresas utilizan una función de desviación automática hacia un servidor aislado para todos los mensajes que superan un determinado volumen. Se informa automáticamente al destinatario de que se ha desviado un mensaje sospechoso hacia este servidor, donde puede consultarlo."

El Documento de Trabajo al que se viene haciendo referencia hace también mención a los principios de exactitud y conservación señalando que "*Este principio requiere que todos los datos legítimamente almacenados por un empleador (después de tener en cuenta todos los demás principios enunciados en este capítulo) que incluyan datos procedentes de una cuenta de correo electrónico de un trabajador, de su utilización de Internet o relativos a las mismas deberán ser precisos y actualizarse y no podrán conservarse más tiempo del necesario. Los empleadores deberían especificar un período de conservación de los mensajes electrónicos en sus servidores centrales en función de las necesidades profesionales. Normalmente, es difícil imaginar que pueda justificarse un período de conservación superior a tres meses."*

Indica también respecto de la seguridad que *"Este principio obliga al empleador a aplicar las medidas técnicas y organizativas adecuadas para proteger todos los datos personales en su poder de toda intromisión exterior. Incluye también el derecho del empleador a proteger su sistema contra los virus y puede implicar el análisis automatizado de los mensajes electrónicos y de los datos relativos al tráfico en la red.*

El Grupo de Trabajo opina que, dada la importancia de garantizar la seguridad del sistema, la apertura automatizada de los mensajes electrónicos no debe considerarse una violación del derecho del trabajador a la vida privada, siempre y cuando existan garantías adecuadas. Por ejemplo, los empleadores pueden ahora utilizar tecnologías que responden a sus intereses en términos de seguridad, pero que no violan el derecho de los trabajadores a la vida privada.

El Grupo de Trabajo «Artículo 29» llama la atención sobre el papel del administrador del sistema, un trabajador cuyas responsabilidades en materia de protección de datos son importantes. Es fundamental que el administrador del sistema, así como cualquier persona que tenga acceso a datos personales de los trabajadores durante las operaciones de control, esté sometido a una obligación estricta de secreto profesional respecto a la información confidencial a la que pueda acceder."

II

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 primero dispone lo siguiente: "1*. La presente Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.*

2*. Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias."*

El artículo 42.2 de la citada Ley 11/2007 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 primero "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."

Establece así, tal y como señala su exposición de motivos, un común denominador normativo que podrá ser completado, mediante objetivos, materialmente no básicos que podrán ser decididos por políticas legislativas territoriales. En este sentido el artículo 11 de dicho Real Decreto 3/2010 establece que "1. *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.(…)*

11.2 A los efectos indicados en el apartado anterior, se considerarán órganos superiores, los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico, de acuerdo con lo establecido en la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado y Ley 50/1997, de 27 de noviembre, del Gobierno; los estatutos de autonomía correspondientes y normas de desarrollo; y la Ley 7/1985, de 2 de abril, reguladora de las bases del Régimen Local, respectivamente.

Los municipios podrán disponer de una política de seguridad común elaborada por la Diputación, Cabildo, Consejo Insular u órgano unipersonal correspondiente de aquellas otras corporaciones de carácter representativo a las que corresponda el gobierno y la administración autónoma de la provincia o, en su caso, a la entidad comarcal correspondiente a la que pertenezcan."

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*."

Por consiguiente, es en el marco de dicha política de seguridad, en el que debe desenvolverse la supervisión de los medios electrónicos puestos a disposición de los empleados públicos para el ejercicio de sus funciones. Dicha supervisión deberá ser respetuosa, con los principios del derecho fundamental a la protección de datos personales.

En particular, la supervisión debe resultar adecuada 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, debiendo analizarse en cada caso si el tratamiento de datos que dicha supervisión comporta 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 supervisión o 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.

Esta Agencia, siguiendo las indicaciones de los instrumentos internacionales antes mencionados, ha venido recomendando 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 del organismo en cuestión o, en su caso, de los habituales en el ejercicio de sus funciones propias de los empleados públicos, 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.

Asimismo, no debe olvidarse que son igualmente principios esenciales del derecho fundamental a la protección de datos los principios de exactitud y conservación recogidos igualmente en el artículo 4, números 3, 4 y 5 de la Ley Orgánica 15/1999 al establecer que "*3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.*

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados."

En consecuencia, además de ser exactos, los datos personales recogidos mediante las medidas de supervisión que se adopten no podrán

mantenerse indefinidamente en los ficheros de la Corporación que ha dictado la norma objeto de consulta, debiendo cancelarse una vez que dichos datos dejen de ser necesarios para la finalidad para la cual fueron obtenidos.

Todo ello sin perjuicio de que las medidas de supervisión o control que se establezcan deban ser igualmente respetuosas de otros derechos fundamentales, tales como el derecho a la intimidad o al secreto de las comunicaciones, cuya protección no corresponde a esta Agencia.