Informe 0233/2009

La consulta plantea diversas cuestiones en relación con la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD) y a su Reglamento de desarrollo, Real Decreto 1720/2007, de 21 de diciembre.

I

En relación con la primera cuestión de consulta, referida a si la forma de llevarse a cabo la entrega de las nóminas a cada trabajador en sobre abierto por un empleado de la comunidad, según consta en el documento de seguridad, constituye una cesión de datos en los términos del artículo 3 i) de la LOPD que define la cesión o comunicación de datos como "toda revelación de datos realizada a una persona distinta del interesado", entendemos que no constituye en sí misma una comunicación de datos a terceros distintos de los afectados, por cuanto no puede presumirse una conducta contraria a la buena fe en el cumplimiento de sus obligaciones laborales por parte de estos empleados, como sería un acceso no permitido al contenido de los sobres, salvo constatación de tal circunstancia, y que, desde la óptica de la protección de datos de carácter personal dicha forma de entrega de las nóminas afectaría al deber de cumplimiento por el responsable del tratamiento de los datos (la propia empresa) de las debidas medidas de seguridad a que viene obligado en aplicación del artículo 9 de la LOPD.

Este artículo señala: "Seguridad de los datos.-1 El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2.-No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas."

Las medidas de seguridad se encuentran reguladas en el Título VIII del Real Decreto 1720/2007, que lleva por rúbrica "De las medidas de seguridad en el tratamiento de datos de carácter personal" y en el Capítulo I dedicado a las Disposiciones generales se contemplan el alcance, los niveles de seguridad y la aplicación de los mismos. Así el artículo 79 establece que "Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento." Por otro lado el artículo 80 determina que "Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.", y por último el artículo 81 regula la aplicación de los niveles de seguridad, estableciendo que:

"1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. (….)"

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros."

Teniendo en cuenta que en las nóminas podrían aparecer datos de afiliación sindical de los trabajadores cuando en ellas aparezca el descuento de la cuota sindical para su transferencia a la organización sindical a la que el trabajador pertenezca, podemos concluir que las medidas de seguridad que debe de adoptar el responsable, que dependerá del tipo de datos al que esté vinculado el fichero o el tratamiento, y que en tanto trata datos de afiliación sindical con la finalidad descrita, deberán ser las medidas de seguridad de nivel básico, reguladas en los artículos 89 a 94, en cuanto en el caso presente se está produciendo un tratamiento automatizado de datos de carácter personal, conforme exige el artículo 81.5 a) señalado.

De modo que, el responsable del fichero de datos debería hacer la entrega de las nóminas en sobre cerrado, aunque la entrega física la realice personal administrativo de la empresa autorizado, impidiendo esta fórmula la pérdida, alteración física, o accesos no autorizados a los datos personales contenidos en su interior por terceras personas.

II

La segunda cuestión que plantea la consultante se refiere a si es procedente la comunicación al Comité de Empresa de los cuadrantes de

servicio mensuales de todos los escoltas de la consultante que están encriptados, y si dicho Comité podría acceder o examinar los mismos fuera de las dependencias de la empresa. Aclara la consultante que el Documento de Seguridad de la empresa permite el acceso a los Representantes Legales de los Trabajadores en las instalaciones, condiciones y medidas de seguridad que recoge el mismo.

En relación con el acceso de los miembros del Comité de Empresa a tales documentos nos encontraríamos, desde la óptica de la protección de datos de carácter personal, ante una cesión o comunicación del artículo 3 i) de la LOPD ya mencionado.

En la materia que nos ocupa, la única cesión prevista de los datos referentes a los trabajadores sería la derivada de las facultades atribuidas a los representantes de los trabajadores es decir, al Comité de Empresa.

En ese caso, tal y como determina el artículo 11.1 de la Ley Orgánica 15/1999, “los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado”. Esta regla de consentimiento sólo se verá exceptuada en los supuestos contemplados en el artículo 11.2, entre los que cabe destacar a) aquellos casos en que una norma con rango de Ley de cobertura a la cesión o el previsto en el apartado c) “cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima cuando se límite a la finalidad que lo justifique.

La posibilidad de cesión de datos referidos a los servicios que prestan mensualmente los trabajadores escoltas, a los representantes sindicales, como consecuencia de la excepción de prestación del consentimiento en los supuestos en que una Ley así lo permita (artículo 11.2.a), debe ponderarse con el legítimo ejercicio de las funciones de control que se atribuyen por la Ley a los órganos de representación colectiva de los trabajadores en la empresa, conforme a las cuales el Estatuto de los Trabajadores dispone que dichos órganos tendrán derecho a acceder a cierta documentación de la empresa en su artículo 64.

En el caso de cesión de los datos de los trabajadores, la misma únicamente podría entenderse amparada en caso de que se produjera en el ámbito de las funciones desarrolladas por los Delegados de Personal o el Comité de Empresa (según sea uno u otro al órgano de representación de los trabajadores), al encontrarse reconocido por el Estatuto de los Trabajadores el derecho de los representantes de los trabajadores (Delegados de Personal o Comité de Empresa) a acceder a determinados datos de los trabajadores en el ámbito de sus competencias. En caso contrario, será necesario el

consentimiento del interesado para proceder a la comunicación de sus datos. De modo que la utilización de los datos por parte de los representantes de los trabajadores debería limitarse a la finalidad de control que a los mismos atribuye el propio Estatuto.

Concretamente, el articulo 64.1, del Estatuto de los Trabajadores, de 24 de marzo de 1995, recoge las competencias del Comité de Empresa y dispone que: "El comité de empresa tendrá las siguientes competencias: Recibir la copia básica de los contratos a que se refiere el párrafo a) del apartado 3 del articulo 8 y la notificación de las prórrogas y de las denuncias correspondientes a los mismos, en el plazo de los diez días siguientes a que tuvieran lugar.", y el apartado 9° atribuye a dicho órgano "Ejercer una labor: a) De vigilancia en el cumplimiento de las normas vigentes en materia laboral, de Seguridad Social y empleo, así como el resto de los pactos, condiciones y usos de empresa en vigor, formulando, en su caso, las acciones legales oportunas ante el empresario y los organismos o tribunales competentes; b) De vigilancia y control de las condiciones de seguridad e higiene en el desarrollo del trabajo en la empresa, con las particularidades previstas en este orden por el artículo 19 de esta Ley".

Cualquier cesión de datos de los trabajadores al Comité de Empresa o Delegados de Personal que exceda de las legalmente previstas en el artículo 64.1 y 9 del Estatuto de los Trabajadores, deberá contar con el consentimiento del interesado, en este caso de los trabajadores afectados.

Pues bien, a nuestro juicio, la función de vigilancia y protección de las condiciones de trabajo, atribuida al Comité de Empresa puede llevarse a adecuado desarrollo sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios como escolta para la consultante. Sólo en el supuesto en que la vigilancia o control se refieran a un sujeto concreto, que haya planteado la correspondiente queja ante el Comité de Empresa, será posible la cesión del dato específico de dicha persona.

En los demás supuestos, la función de control quedará plenamente satisfecha, a nuestro juicio, mediante la cesión al Comité de información debidamente disociada, según el procedimiento definido en el artículo 3 f) de la Ley Orgánica 15/1999, que permita a aquél conocer las circunstancias cuya vigilancia le ha sido encomendada sin referenciar la información en un sujeto concreto.

En consecuencia, procederá, en caso de haber sido formalmente solicitada, la cesión de los datos solicitados, siempre que los mismos sean cedidos de forma disociada, sin poder referenciar los datos a personas identificadas o identificables. En caso contrario, deberá recabarse el consentimiento de los interesados, conforme exigen los artículos 11 y 21 de la Ley Orgánica 15/1999.

Por último, a los solos efectos informativos, debe recordarse que el artículo 11.5 de la Ley Orgánica 15/1999 dispone que "Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley".

Ello conlleva una serie de conclusiones en relación con la actuación que deberá llevar a cabo el Comité de Empresa una vez recibidos los datos:

En primer lugar, la comunicación a los órganos de representación de los trabajadores únicamente puede considerarse adecuada, conforme al artículo 4.1 de la LOPD, dentro de las funciones de control que al mismo atribuye el Estatuto de los Trabajadores. Por ello, cualquier utilización de los datos para una finalidad distinta de la citada o su posterior divulgación podría resultar contraria a lo dispuesto en la Ley Orgánica 15/1999, por vulneración de lo dispuesto en el citado artículo 4.2. Además, la divulgación podría incluso implicar una cesión de datos que debería encontrarse amparada por lo dispuesto en el artículo 11 de la citada Ley. Debe recordarse que el artículo 10 de la LOPD establece el deber de secreto profesional del responsable del fichero y de quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal y el deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Asimismo en caso de que el Comité conserve los datos comunicados, incorporándolos a un fichero deberá dar cumplimiento a la obligación de seguridad impuesta por el artículo 9 de la Ley Orgánica 15/1999.

Por otra parte, vista la posibilidad de que los miembros del Comité accedan a los datos personales en los términos analizados, debe señalarse que el artículo 88 del Reglamento establece en su número 1: "El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente, que será de obligado cumplimiento para el personal con acceso a los sistemas de información."

En su número 3 señala el contenido mínimo del mismo que, entre otras, deberá (apartado b) especificar las medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento. Y (apartado c) las funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

Así pues, el acceso a los datos solicitados por el Comité deberá hacerse en las condiciones que señala su Documento de Seguridad que, según la consultante, permite el acceso a los datos en las dependencias de la empresa, teniendo en cuenta, además, que el artículo 86 del Reglamento regula el régimen de trabajo fuera de los locales del responsable del fichero o encargado

del tratamiento estableciendo lo siguiente: “1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o un perfil de usuarios y determinando un período de validez para las mismas.”

II

La consulta plantea además diversas dudas relativas a la adecuación a la normativa de protección de datos de la instalación de cámaras de videovigilancia en aulas de formación en el centro de trabajo con la finalidad de controlar la efectiva asistencia a las acciones formativas.

La primera cuestión que resulta de la consulta es la relativa a la legitimación para el tratamiento de imágenes, por lo que debe considerarse si es preciso el consentimiento inequívoco de los trabajadores para la instalación de cámaras de videovigilancia en el centro de trabajo. A este respecto la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras, remite en su artículo 2 a lo previsto en el artículo 6.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD) donde se establece que “*el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa*”, sin perjuicio de que dicho consentimiento podrá quedar excluido, de acuerdo con lo dispuesto por el artículo 6.2 cuando, el tratamiento sea necesario para el adecuado desenvolvimiento de la relación laboral de los trabajadores con la empresa.

A mayor abundamiento respecto del tratamiento de datos de imágenes en el lugar de trabajo, el artículo 20.3 del el Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (en adelante ET) dispone 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”.*

Por otra parte, no se puede obviar la doctrina del Tribunal Supremo, en Sentencia de 18 de junio de 2006 en virtud de la cual dichas medidas (como las relacionadas con la utilización de Internet y correo electrónico) deben haber

sido hechas constar expresamente al trabajador, pasando así a formar parte de la propia relación laboral y siendo el tratamiento de los datos necesario para su adecuado desenvolvimiento.

De todo ello se desprende que la aplicación del artículo 20.3 ET no legitima por sí solo el tratamiento de las imágenes, si bien este será posible, aún sin contar con el consentimiento del afectado en caso de que el trabajador haya sido debidamente informado de la existencia de esta medida, debiendo además ser claro que, conforme a lo exigido por el artículo 4.2 LOPD, los datos no podrán ser utilizados para fines distintos.

La información constituye en uno de los elementos esenciales para garantizar el derecho fundamental de protección de datos. La Audiencia Nacional ha señalado en sentencia de 15 de junio de 2001 que "*se trata de un derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos, y así lo valora el texto positivo al pormenorizar su contenido y establecer la exigencia de que el mismo sea expreso, preciso e inequívoco."*

Por tanto el tratamiento de las imágenes por el responsable del tratamiento, le obliga a cumplir con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD que dispone, "los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".

En cuanto al modo en que haya de facilitarse dicha información, debe tenerse en cuenta que en el ámbito laboral además de la información personalizada a los trabajadores de la que deberá quedar la adecuada constancia, exigirá su comunicación a los representantes de los trabajadores, en tanto que el artículo 64.1 ET dispone que "*El comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores…"* y en el punto 5 que *" El comité de empresa tendrá derecho a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por éste, sobre las siguientes cuestiones:*

f) La implantación y revisión de sistemas de organización y control del trabajo, estudios de tiempos, establecimiento de sistemas de primas e incentivos y valoración de puestos de trabajo."

Asimismo, debe tenerse en cuenta la específica modalidad de información en materia de videovigilancia que recoge el artículo 3 de la Instrucción 1/2006

"*Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:*

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción."

Todo ello en aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.