12.7.2010

COMUNICACIÓN A LOS MIEMBROS

Asunto: Petición 1198/2009, presentada por J. F. K., de nacionalidad húngara, sobre la invasión del ámbito privado de los trabajadores por parte de empresas multinacionales

1. Resumen de la petición

El peticionario se queja de la práctica llevada a cabo por empresas multinacionales de registrar los bolsos de los empleados después del trabajo, de la vigilancia por videocámaras durante la jornada laboral y de la necesidad de presentar un currículum vítae a la hora de solicitar empleo. Considera que ello constituye una violación de los derechos humanos y solicita al Parlamento Europeo que tome medidas para subsanar la situación.

2. Admisibilidad

Admitida a trámite el 1 de diciembre de 2009. Se pidió a la Comisión que facilitara información (artículo 202, apartado 6, del Reglamento).

3. **Respuesta de la Comisión**, recibida el 12 de julio de 2010

La petición

El peticionario se queja de los tres tipos de prácticas que ciertas empresas multinacionales, tales como Jabil, Nokia y Sanmina, llevan a cabo en Hungría: 1) el registro de lo bienes personales de los empleados (e incluso, con frecuencia, cacheos) por parte de los guardias de seguridad en las instalaciones de las empresas multinacionales; 2) la obligación de remitir un currículum vítae por adelantado cuando se solicita trabajo; y 3) la vigilancia ofensiva por videocámara en el lugar de trabajo. El peticionario señala que no dispone de pruebas para justificar sus acusaciones, pero explica que los empleados tienen que firmar un acuerdo especial por el que se comprometen a no utilizar teléfonos móviles o cámaras en el lugar de

trabajo. Asimismo, el peticionario manifiesta que existen normas por las que las imágenes y el sonido para grabaciones de video o audio no pueden reproducirse de manera ofensiva mediante el acoso a terceras personas ni efectuarse en contra de su voluntad. En casos de extrema necesidad, y por razones debidamente justificadas, se puede realizar una grabación a efectos de prueba.

El peticionario considera que dichos registros son humillantes; que la obligación de remitir su currículum vítae por adelantado constituye una recopilación ilícita de datos; y que la prohibición de utilizar un teléfono con cámara en su lugar de trabajo representa una violación de los derechos humanos. Así pues, el peticionario solicita que se apliquen los instrumentos jurídicos necesarios para proteger a los empleados de las prácticas que se mencionan con anterioridad.

Comentarios de la Comisión sobre la petición

La Directiva relativa a la protección de datos (Directiva 95/46/CE[1]) establece el marco jurídico para el tratamiento de datos personales en todos los Estados miembros. En caso de que un Estado miembro no haya cumplido la obligación de aplicar la Directiva, los ciudadanos pueden solicitar la aplicación directa de determinadas disposiciones de la misma. En este sentido, el Tribunal de Justicia de la Unión Europea dictaminó en el asunto C-465/00[2] que algunas disposiciones tienen un efecto directo, tales como el artículo 6, apartado 1, letra c) (principios relativos a la calidad de los datos: los datos han de ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente), y el artículo 7, letras c) y e) (principios relativos a la legitimación del tratamiento de datos).

La Directiva es aplicable únicamente a los datos personales que se inscriban en su ámbito de aplicación. El artículo 2 define «datos personales» como «toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

La Directiva 95/46/CE establece los principios que toda actividad de tratamiento de datos debe cumplir para considerarse lícita. Asimismo, otorga ciertos derechos a aquellas personas cuyos datos son tratados, con el fin de garantizar el derecho fundamental a la protección de los datos personales. Los principios consagrados en el artículo 6 constituyen el fundamento de la protección de los datos personales, puesto que se refieren a la calidad de los datos cuando son tratados: la recogida y el tratamiento de los datos personales deben realizarse con fines determinados y explícitos (principio de limitación de los fines); los datos personales deben ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente (principio de proporcionalidad); y los datos personales deben actualizarse cuando sea necesario. Asimismo, el tratamiento de datos personales debe

[1] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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, DO L 281 de 23.11.1995, p. 31.

[2] Sentencia del TJUE en los asuntos acumulados C-465/00, C-138/01 y C-139/01: Rechnungshof y Österreichischer Rundfunk, apartados 98 y siguientes.

efectuarse durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

En virtud de lo dispuesto en el artículo 7, el tratamiento de datos se considera legítimo únicamente si:

a) el interesado ha dado su consentimiento de forma inequívoca, o
b) es necesario para la ejecución de un contrato vinculante para el interesado, o
c) es necesario para el cumplimiento de una obligación jurídica, o
d) es necesario para proteger el interés vital del interesado, o
e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público, o
f) es necesario para la satisfacción del interés legítimo de una persona física o jurídica, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.

El interesado tiene derecho a ser informado sobre el tratamiento de sus datos personales, a acceder a los datos, a solicitar la rectificación, la supresión o el bloqueo de los mismos, así como a obtener una reparación efectiva por los daños sufridos a raíz de un tratamiento ilícito de sus datos. Estos derechos podrán restringirse en la medida en que sea estrictamente necesario no solo para salvaguardar la seguridad del Estado y la defensa, sino también para realizar investigaciones y entablar procedimientos penales.

La supervisión y el control de las actividades de tratamiento de datos corresponden a las autoridades de control públicas independientes (artículo 28), normalmente denominadas «autoridades de protección de datos», que son las autoridades competentes para velar por que todo tratamiento de datos personales a nivel nacional se efectúe de conformidad con la legislación nacional de transposición de la Directiva.

Para que la Directiva 95/46/CE relativa a la protección de datos sea de aplicación, se han de comprobar los dos aspectos que se describen a continuación.

El aspecto más importante está relacionado con los datos tratados y si estos se entienden en el sentido de «datos personales» tal y como se definen en el artículo 2, letra a). En lo que respecta a la segunda y tercera práctica que denuncia el peticionario, los datos que se incluyen en un currículum y que se graban a través de un sistema de videovigilancia se consideran datos personales en el sentido de la Directiva 95/46/CE. En lo que respecta a la primera práctica que denuncia el peticionario, los cacheos no entran en el ámbito de aplicación de la Directiva relativa a la protección de datos.

El segundo aspecto relevante se refiere a la persona que efectúa el tratamiento de datos personales. Tanto el responsable como el encargado del tratamiento de datos deben cumplir una serie de obligaciones. Las empresas multinacionales, tales como Jabil, Nokia y Sanmina, son personas jurídicas que determinan independientemente el fin y los medios del tratamiento de los datos personales que recogen, como por ejemplo los datos incluidos en un currículum vítae o los datos grabados mediante un sistema de videovigilancia. Así pues, se considera que estas empresas son los responsables del tratamiento tal y como se define en la Directiva 95/46/CE, aunque puedan delegar o subcontratar el tratamiento de los datos personales a los encargados, quienes llevarán a cabo dicha tarea en su nombre.

Primera acusación: registro a los empleados (e incluso, con frecuencia, cacheos) por parte de los guardias de seguridad

De conformidad con el Tratado de la Unión Europea y el Tratado de Funcionamiento de la Unión Europea, la Comisión Europea no tiene competencias para intervenir en casos concretos de supuestas violaciones de los derechos fundamentales. La Comisión podrá intervenir únicamente en aquellos casos relacionados con la legislación de la UE.

En relación con la denuncia del peticionario sobre los registros a los empleados (e incluso, con frecuencia, cacheos) por parte de los guardias de seguridad en las fábricas de montaje, cabe mencionar que no existe legislación específica de la UE relativa a este asunto. Por tanto, la Comisión no puede continuar el trámite de este asunto.

Segunda acusación: obtención ilícita de datos mediante la solicitud del currículum vítae a un posible futuro empleado

En la actualidad, los puestos vacantes de una empresa se ocupan tras un proceso de selección de candidatos interesados e idóneos para dichos puestos. En general, este proceso incluye una fase de preselección que se lleva a cabo en función de los currículos que los candidatos interesados remiten con antelación. El tratamiento de los datos contenidos en los currículos se inscribe en el ámbito de aplicación de la Directiva 95/46/CE relativa a la protección de datos y está sometido a los principios de legitimidad, necesidad y proporcionalidad (artículo 6 de la Directiva).

En la mayor parte de los casos, el tratamiento de los datos incluidos en los currículos puede justificarse como legítimo puesto que:

- se efectúa con el consentimiento del interesado (artículo 7, letra a)), o
- es necesario para la ejecución de un contrato de trabajo entre el empresario y el empleado (artículo 7, letra b)), o
- es necesario para la satisfacción del interés legítimo perseguido por el empresario para conocer las cualificaciones de los posibles empleados y así escoger a la persona más idónea para el puesto vacante (artículo 7, letra f)).

El tratamiento de los datos personales incluidos en los currículos debe ser proporcionado a los fines legítimos que se persiguen y debe ofrecer, en particular, los medios menos intrusivos posibles. Dado que se establecen suficientes garantías, el tratamiento de dichos datos para los mencionados fines estaría en consonancia con la Directiva 95/46/CE. Estas garantías pueden incluir, entre otros, las siguientes prácticas:

- informar a los empleados de la identidad del responsable del tratamiento y de los fines de la vigilancia, así como facilitar cualquier información suplementaria que resulte necesaria para garantizar un tratamiento de datos leal con respecto al interesado (artículo 11);

- informar al interesado del derecho de rectificación de los datos que le conciernen y del derecho de supresión de los datos, en particular, cuando no se ha obtenido el puesto de trabajo solicitado.

El mero hecho de que un empresario solicite una copia del currículum vítae por adelantado a un posible futuro empleado no puede considerarse como una recopilación ilícita de datos, tal y como afirma el peticionario.

Tercera acusación: vigilancia por videocámara en el lugar de trabajo

La videovigilancia se inscribe en el ámbito de aplicación de la Directiva 95/46/CE relativa a la protección de datos. Los principios de la protección de datos, en particular los principios de legitimidad, necesidad y proporcionalidad (artículo 6 de la Directiva) se aplican a todo tratamiento de datos personales obtenidos mediante un sistema de videovigilancia.

El Grupo de trabajo del artículo 29[1] ha presentado dos opiniones en relación con la videovigilancia en el lugar de trabajo[2], en las que se definen las directrices para aplicar las disposiciones de la Directiva relativa a la protección de datos a la videovigilancia. Con arreglo a estas opiniones, la legalidad de la videovigilancia en el lugar del trabajo depende de varios factores:

En primer lugar, el objetivo del tratamiento: los sistemas de videovigilancia pueden justificarse si su instalación, sometida a las garantías adecuadas, se realiza con el fin de satisfacer los requisitos de protección y seguridad en el lugar de trabajo o por razones de seguridad. Los diferentes intereses en juego deben tenerse en cuenta caso por caso y en el contexto específico en el que se encuentran.

La instalación de sistemas de videovigilancia en empresas por motivos de protección y seguridad en el trabajo (para evitar el robo de dispositivos electrónicos o la apropiación de información de investigaciones tecnológicas) puede ser legítima, siempre que sea necesario para la satisfacción del interés legítimo de dichas empresas (los responsables del tratamiento) para garantizar la seguridad de las instalaciones y evitar la apropiación de información de investigaciones tecnológicas y de secretos comerciales, y siempre que los intereses de los empleados prevalezcan al interés de las empresas (artículo 7, letra f)).

También se puede justificar el uso de los sistemas de videovigilancia para proteger el interés vital del interesado, por ejemplo por motivos de seguridad en el lugar de trabajo, entre otros, en caso de accidentes durante la producción (artículo 7, letra d)).

En segundo lugar, la necesidad y la proporcionalidad del tratamiento: la instalación de un sistema de videovigilancia deber ser proporcionada a los fines legítimos que se persigan y debe utilizar los medios de tratamiento menos intrusivos posibles. Los intereses del empresario de instalar un sistema de videovigilancia deben estar en equilibrio con los

[1] El grupo de protección de las personas en lo que respecta al tratamiento de datos personales (el «Grupo») se creó en virtud del artículo 29 de la Directiva 95/46/CE relativa a la protección de datos. El Grupo está compuesto por los representantes de las autoridades nacionales de protección de datos de cada Estado miembro. El Grupo ejerce sus funciones con plena independencia y tiene carácter consultivo con respecto a la Comisión.

[2] Opinión 8/2001 (WP48) sobre el tratamiento de datos personales en el contexto del empleo, Documento de trabajo de 25 de noviembre de 2002 (WP67) sobre el tratamiento de datos personales a través de sistemas de videovigilancia y Opinión 4/2004 (W89) sobre el tratamiento de datos personales a través de sistemas de videovigilancia.

intereses del empleado de obtener la protección necesaria de sus datos personales. Esto se puede conseguir únicamente si se establecen las garantías adecuadas; solo entonces la videovigilancia estará en consonancia con la Directiva 95/46/CE. Dichas garantías podrían incluir, entre otros, las siguientes prácticas:

- prohibir la instalación de sistemas de videovigilancia en cuartos de baños, duchas, armarios y zonas de descanso;

- informar a los empleados sobre la identidad del responsable del tratamiento y sobre los fines de la videovigilancia, así como facilitar cualquier información suplementaria que resulte necesaria para garantizar que un tratamiento se efectúa de forma leal con respecto al interesado;

- reducir el tiempo de conservación de los vídeos;

- efectuar un control independiente por parte de las autoridades nacionales de protección de datos que son competentes para velar por el cumplimiento de la legislación nacional de transposición de la Directiva 95/46/CE y para establecer las garantías y los requisitos adecuados para la licitud del sistema.

En último lugar, el responsable del tratamiento tiene la obligación (artículo 11) de informar, de manera visible, clara y explícita, a las personas que entren en un lugar equipado de un sistema de videovigilancia, de que están siendo grabadas. En el caso de que los sistemas de videovigilancia se instalen en el lugar de trabajo, los representantes de los trabajadores también deben ser informados.

Conclusiones

Con respecto a la primera acusación sobre los registros a empleados (en particular, los cacheos), la Comisión no puede continuar con el asunto, puesto que no se incluye en el ámbito de aplicación de la legislación de la UE.

Con respecto a las otras acusaciones, el peticionario no presentó ninguna prueba que demuestre que las filiales de las multinacionales Jabil, Nokia y Sanmina han infringido la Directiva 96/45/CE.

Se invita al peticionario a que presente cualquier queja en relación con estas multinacionales, y que estén relacionadas con la vulneración de sus derechos de protección de datos, a la autoridad nacional de protección de datos de Hungría:

Comisario de protección de datos de Hungría
Nádor u. 22
1051 Budapest
Tel: +361 4757100 / +361 4757186
Fax: +361 2693541
E-mail: adatved@obh.hu