Informe 0201/2010

La consulta plantea la viabilidad jurídica de la creación a través de una web de una base de datos común a la que sólo tendrían acceso las empresas asociadas a la consultante que asumirían el compromiso de aportar los datos de carácter personal de sus trabajadores con su consentimiento y con la finalidad de poder comprobar los datos de los candidatos a ofertas de empleo de dichas empresas asociadas, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

I

En el sistema descrito, cada una de las empresas que decidieran asociarse a la consultante para hacer uso de la base de datos común, sería responsable del fichero de sus respectivos trabajadores, asumiendo la consultante la condición de responsable de la página web donde consultar el fichero o base de datos común, atendiendo a la definición que el artículo 3 d) de la LOPD da del responsable del fichero o tratamiento "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

Según se deduce de la consulta, las empresas asociadas usuarias de esta base de datos común aparecerían identificadas mediante la asignación de una clave individualizada de usuario mediante cifrado individual de identidad (código operativo), trazabilidad y marca electrónica de la consulta que no podrían reproducir, lo que indica que estaríamos ante un acceso a la web restringido a las empresas asociadas y no general.

Los datos personales de sus empleados que las empresas deberían aportar a esta base no comprenderían datos sensibles (afiliación sindical o salud) ni datos relativos a la remuneración y situación familiar. No obstante, entre los datos que las empresas suministrarían figuran un código identificativo de la causa de suspensión o extinción de la relación laboral, existencia de reclamaciones judiciales contra la empresa efectuadas por el trabajador, así como si es susceptible de nueva contratación en función de respuestas a preguntas que no se concretan, extremos estos últimos que pueden afectar negativamente a la reputación del trabajador y a su futura empleabilidad, lo que convertiría a la base de datos común accesible por Internet por las empresas asociadas en una lista negra.

La primera cuestión que resulta de la consulta formulada se refiere a qué debe entenderse por lista negra al no existir en nuestro derecho un concepto legal al que acudir. A este respecto, 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 documento de trabajo sobre las listas negras de 3 de octubre de 2002, ha abordado de forma genérica un posible concepto básico de lista negra configurándola como "*la recogida y difusión de determinada información relativa a un determinado grupo de personas, elaborada de conformidad con determinados criterios dependiendo del tipo de lista negra en cuestión, que generalmente implica efectos adversos y perjudiciales para las personas incluidas en la misma, que pueden consistir en discriminar a un grupo de personas al excluirlas de la posibilidad del acceso a un determinado servicio o dañar su reputación.*"

Señala, este documento, que dado que cualquier operación o conjunto de operaciones aplicadas a datos personales constituye un tratamiento de datos personales sujeto a la Directiva 95/46 CEE y a las respectivas normativas en materia de protección de datos en cada Estado miembro, para que las listas negras puedan existir legalmente deberán someterse a los principios de legitimación que aparecen en dicha Directiva y respetar los derechos que a los ciudadanos les confiere la misma, salvo que puedan acogerse a alguna de las excepciones previstas en ella.

La traslación de estos principios al derecho español se encuentra en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, según el cual *"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.*

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando 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; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado."

De esta manera, salvando aquellos supuestos en que las listas negras tienen de alguna manera una base legal, como sucede en el derecho español con los ficheros de solvencia patrimonial y crédito regulados en la propia Ley

Orgánica 15/1999 y cuyo fundamento se encuentra en el interés legítimo de preservación y estabilidad del sistema financiero, o se encuentran legitimadas en alguno de los supuestos previstos en el artículo 6.2 de la Ley Orgánica 15/1999, la inclusión de datos personales en un lista negra requeriría el consentimiento del interesado para ser conforme a lo dispuesto en la normativa de protección de datos.

II

Por otra parte, la cuestión de quien resulta responsable de la página web en la que obra este fichero común resulta esencialmente relevante, ya que será la entidad responsable la que, en lo que se refiere al tratamiento consistente en la recogida y organización de los datos se encuentre directamente obligada a acreditar el cumplimiento de las obligaciones legalmente previstas, esencialmente en lo relativo a la recogida del consentimiento de los afectados y el cumplimiento del deber de información a los mismos, en los términos recogidos en el artículo 5 de la Ley Orgánica 15/1999. Asimismo, sería esta entidad responsable, y no la totalidad de las posibles usuarias del sistema, quien debería proceder a la inclusión y actualización de los datos en el fichero, cumpliendo así con el principio de exactitud de los datos recogido en el artículo 4.3 de la LOPD que dice que “Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado”. Esta obligación de actualización de los datos que corresponde a cada empresa responsable del fichero de sus empleados, se extiende al responsable del fichero común cesionario de los datos. Así el artículo 8.5 del Reglamento contempla que “Cuando los datos hubieran sido comunicados previamente el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación o cancelación.”

Asimismo, el responsable del fichero común deberá notificar (para su inscripción en el Registro General de la Agencia de Protección de Datos) la creación de dicho fichero, de acuerdo con lo previsto por el artículo 25 de la referida Ley Orgánica, garantizando a los afectados por el tratamiento, los derechos de acceso, rectificación, oposición y cancelación a los que se refieren los artículos 15 y 16 de dicha norma.

III

Por otra parte, el sistema planteado implicará la existencia de múltiples cesiones de datos a la entidad que resulte ser responsable de la web y de ésta a aquellas que sean “usuarias” del sistema.

Cualquier acceso a los datos entre las diferentes empresas que accedan a la base común constituye un supuesto de cesión definida en el artículo 3 i) de la LOPD como ”toda revelación de datos realizada a una persona distinta del interesado”, que requiere el consentimiento de los afectados o una habilitación legal para la misma.

De este modo, será preciso, en primer lugar, que la cesión se encuentre amparada en el consentimiento del afectado, dado que el artículo 11.1 de la Ley Orgánica 15/1999 dispone que “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”. Este consentimiento deberá ser debidamente informado, indicándose claramente quiénes podrán ser destinatarios de los datos, lo que obligará a que, en caso de que para la cesión se utilicen canales como Internet, se establezcan mecanismos que garanticen que la información no será libremente accesible a través de un determinado sitio web, sino que se limiten las personas y entidades que podrán acceder a la información, a través de las correspondientes medidas que permitan lograr dicha restricción. En consecuencia, teniendo en cuenta la finalidad perseguida por el sistema, no procedería sin más la inclusión de los datos en un sitio web sin la adopción de tales medidas.

El consentimiento del interesado sólo se verá exceptuado en los supuestos contenidos en el artículo 11.2, cuyo apartado c) prevé expresamente la posibilidad de proceder a la cesión inconsentida “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 en cuanto se limite a la finalidad que la justifique”. A nuestro juicio, el supuesto contemplado no encajaría en este apartado c), pues la relación entre empresa y trabajador no implica necesariamente la conexión con el fichero del consultante. Por ello, el consentimiento del trabajador deberá ser otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11.3), y que debe recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder.

Tal como advierte la consultante, el consentimiento para la cesión de los datos de sus trabajadores se recogería por cada empresa al formalizar el contrato o durante la relación laboral.

En lo que se refiere a la prestación del consentimiento, el artículo 3 h) de la LOPD define dicho consentimiento como “una manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”. Un adecuado análisis del concepto exigirá poner de manifiesto, cuál es a juicio de esta

Agencia la interpretación que ha de darse a estas cuatro notas características del consentimiento. La Agencia Española de Protección de Datos ha venido sosteniendo los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa, que el consentimiento habrá de ser:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

b) Específico, es decir referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la Ley Orgánica 15/1999.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la Ley Orgánica impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

De modo que para que no sea nulo, el consentimiento que se solicita a los empleados, se deberá facilitar a éstos la información que les permita conocer la finalidad a la que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad del cesionario.

Dicho consentimiento tiene también el carácter de revocable (artículo 11.4).

Como regla general, corresponde al responsable del fichero común, estar en condiciones de acreditar que ha obtenido el consentimiento para el tratamiento de los datos, y a la empresa que cede los datos al fichero común la prueba del consentimiento para la cesión de los mismos. De nuevo el artículo 12.2 del Reglamento dice que “Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.” Indicando en su número 3 que “Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.”

IV

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 en 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 solamente 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.

En nuestro caso, no cabe duda de que del conjunto de datos a ceder por las empresas puede contribuir a configurar un perfil del trabajador que puede

producirle algún tipo de discriminación en el acceso o mantenimiento de un empleo, teniendo en cuenta que entre los datos figuran los relativos a la suspensión por posibles sanciones o huelgas y a la litigiosidad originada por el trabajador con sus demandas contra la empresa.

En el ámbito de la Unión Europea, destacan importantes Documentos de Trabajo del "Grupo del Artículo 29", constituido al amparo de la Directiva 95/46, de 24 de octubre, sobre Protección de Datos, de la cual es una transposición la Ley Orgánica 15/1999, 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 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. En nuestro caso, la finalidad de la cesión a la base de datos común que parece ser la de empleo, determina que todos aquellos datos del trabajador que pudieran cederse y utilizarse en perjuicio de sus posibilidades de empleo, resultarían inadecuados innecesarios y

desproporcionados para tal fin, siendo ilegítimo el tratamiento o cesión de datos de los trabajadores con fines discriminatorios para el empleo de éstos.

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.

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. Libertad de expresión que resulta difícil de entender cuando los datos a ceder pueden ser utilizados en su contra.

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.

De lo señalado anteriormente, cabe concluir que el consentimiento para la comunicación por Internet de los datos de sus empleados, incluidas las evaluaciones sobre los mismos, no podría entenderse válidamente prestado en el contexto de la relación laboral si su negativa a darlo, llevase aparejada algún tipo de consecuencia adversa o discriminatoria, no pudiendo hablarse de consentimiento libre.

Por ello, entendemos que la comunicación de los datos de empleados en Internet, no puede ampararse en el consentimiento del trabajador, en el ámbito de la relación laboral.

V

Por último señala la consultante que los datos de carácter personal permanecerán en la base de datos común durante dos años, aplicándose al fichero común las medidas de seguridad de nivel alto.

El plazo de conservación de los datos de carácter personal objeto de tratamiento debe responder al principio de calidad de los datos recogido por el artículo 4.5 de la LOPD que dice que “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”

Pues bien, teniendo en cuenta que la cesión de los datos señalados por el consultante no podría entenderse amparada en el consentimiento libre de los trabajadores, y en la medida en que la base de datos común pudiera tener efectos adversos para el empleo y relación laboral de los afectados titulares de los datos, esto es, podría considerarse una “lista negra de trabajadores”, no procedería la creación a través de la web de la consultante de la base de datos que propone en su escrito.

Como consecuencia de lo señalado, carece de sentido un pronunciamiento sobre el plazo de conservación de los datos.