Boletín social Quantor

Avance de información social

Selección de las cuestiones más relevantes de la actualidad social

[Quantor]

Número 90 · abril 2008

[Artículo de opinión]

La protección de los datos de los trabajadores en el nuevo reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal

Ernesto José Muñoz Corral

Abogado - Socio. Picón & Asociados

Introducción

La entrada en vigor, el 19 de abril del año en curso, del esperado Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), **QS 2007/28045**, supone un importante hito en la regulación normativa de una materia tan sensible como de actualidad: la tutela del derecho fundamental a la protección de datos personales.

Hasta la aparición de la nueva norma, la regulación de este ámbito se basaba en una legislación de desarrollo desfasada y caduca, surgida al amparo de una Ley ya derogada (la Ley Orgánica 5/1992, de 24 de octubre, reguladora del tratamiento automatizado de datos de carácter personal) y que el legislador había mantenido vigente de modo pretendidamente coyuntural.

La aprobación del Reglamento se justifica porque las normas hasta hace poco subsistentes habían quedado obsoletas frente a la desbordante evolución tecnológica y social experimentada en los últimos años, lo que demandaba una adaptación a las circunstancias actuales. Además, se hacía necesario corregir las carencias que, a lo largo de estos años, se han puesto de manifiesto en la aplicación práctica de los Reglamentos derogados, introduciendo criterios interpretativos y modificaciones orientadas a, por una parte, facilitar el cumplimiento de la legalidad y, por otra, aclarar ciertos conceptos oscuros que ponían en entredicho las garantías propias del principio de seguridad jurídica.

La regulación contenida en el Reglamento tiene singular relevancia en el ámbito de la protección de los datos personales de los trabajadores, aspecto este que plantea su propia y peculiar problemática. Analizaremos en las siguientes páginas la aplicación de la nueva normativa a este concreto y sensible campo.

En este número:

[1] Artículo de opinión

La protección de los datos de los trabajadores en el nuevo reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal

Ernesto José Muñoz Corral

[6] La jurisprudencia responde

La calificación del despido por enfermedad del trabajador: una cuestión zanjada, al menos judicialmente

Ricardo Morón Prieto

[9] Últimos Convenios colectivos publicados

Del 1 al 31 de marzo de 2008

[15] La jurisprudencia más reciente

[16] Esquemas básicos

Creación de ficheros de empleados

Con carácter general, el Reglamento mantiene la exigencia de que, antes de la contratación de los trabajadores, la empresa deberá inscribir un fichero de empleados en el Registro General de la Agencia Española de Protección de Datos (AEPD), órgano administrativo de fiscalización y control en esta materia. Dicha inscripción será presupuesto previo para la legalidad del tratamiento de los datos personales.

A los efectos de la inscripción, únicamente se comunicarán a la AEPD las características generales del fichero (tipología de los datos, finalidad, cesiones previstas, etc.), pero no los concretos datos personales de los empleados, por lo que la contratación de nuevos trabajadores o las bajas de los ya existentes no harán necesario introducir modificaciones en la inscripción del fichero.

Aunque de ordinario los datos de los trabajadores serán tratados por el empresario tanto en soporte informático como en papel, no será necesario comunicar dos ficheros distintos a la AEPD, sino que podrá inscribirse un único fichero de empleados, haciendo constar que de él se hace un tratamiento mixto.

Datos excluidos del ámbito de protección del Reglamento

El Reglamento introduce una importante novedad en esta materia y excluye del régimen de aplicación de la protección de datos de carácter personal los dos siguientes tipos de datos:

- Los datos personales de empresarios individuales, siempre que se traten en su calidad de comerciantes, industriales o navieros.
- Los datos relativos a personas físicas que presten sus servicios en personas jurídicas (entidades privadas o administraciones públicas), siempre que los datos tratados se limiten a su nombre y apellidos, funciones o puestos desempeñados y dirección postal o electrónica, teléfono y fax profesionales.

Lo anterior implica que, en principio, el nuevo Reglamento está excluyendo de su ámbito de protección los tradicionales ficheros de contactos y de proveedores que, probablemente, mantienen la totalidad de las empresas.

Ello tiene especial relevancia en el ámbito que nos ocupa, ya que, frecuentemente, los datos de contacto de clientes y proveedores son datos de trabajadores de la empresa cliente o proveedora. Pues bien, estos datos que, al amparo de la normativa derogada, solían tutelarse de igual modo que el resto de datos de carácter personal, conforme a la nueva regulación podrán ser tratados sin que haya que aplicarles las garantías de la protección de datos personales.

No pocas dudas surgen al contemplar esta novedosa previsión, ya que la LOPD, preeminente en virtud del principio de jerarquía normativa, no recoge en modo alguno la excepción al régimen protector que prevé el Reglamento.

Aplicación de los principios de la protección de datos a los datos de trabajadores

Principio de Calidad

Recabados los datos del trabajador en el ámbito de una relación laboral, los datos incorporados a los ficheros de la empresa deben ser únicamente aquellos que resulten adecuados, pertinentes y no excesivos para la formalización, desarrollo y cumplimiento de la relación laboral, es decir, para la gestión de recursos humanos,

Directora Editorial: Sol Mena del Río.
Jefa de Sección Social: Raquel Ruiz Ortega.
Redacción: Silvia Ausín García, Ana González Ruiz, Julia de Isusi García, Ana Mendívil Herrera.
Director Comercial: Luis Ortiz Olmeda.
Director de Marketing: Íñigo de Juan Sainz-Planillo.

[Quantor]
Grupo Editorial

pago de las nóminas, gestión de seguros sociales, etc. Además, dichos datos han de ser utilizados exclusivamente para satisfacer dichas finalidades y no otras

Puesto que el tratamiento de los datos de los trabajadores por el empresario se fundamenta en la existencia de una relación laboral, una vez extinguida esta, los datos deben ser cancelados de oficio por la empresa, si bien podrán conservarse bloqueados durante el tiempo en que tarden en prescribir las eventuales responsabilidades que pudieran derivarse de la relación mantenida con el trabajador.

Consentimiento

Como regla, para poder llevar a cabo el tratamiento o la cesión a terceros de los datos de una persona, es necesario obtener su consentimiento previo. Este consentimiento no será necesario cuando exista una Ley que habilite u obligue a efectuar el tratamiento o cesión de datos o cuando estos sean tratados en el marco de un contrato, precontrato o de una relación jurídica, negocial, laboral o administrativa cuyo cumplimiento, desarrollo o control haga necesario el tratamiento.

El empresario no necesitará obtener el consentimiento del trabajador para tratar sus datos personales en el ámbito de la relación laboral, ni para cederlos a tercero cuando dicha cesión venga impuesta por la Ley. Dicho consentimiento no será necesario, por ejemplo, para llevar a cabo la elaboración y pago de las nóminas, la gestión de seguros sociales o la comunicación de los datos del empleado a la Hacienda Pública o a los Organismos de la Seguridad Social.

Ahora bien, la no exigencia del consentimiento del trabajador para el tratamiento de sus datos personales por el empresario se limita a aquellas finalidades que vengan impuestas por la Ley o que sean necesarias para el mantenimiento y cumplimiento de la relación laboral. El empresario no podrá utilizar los datos del trabajador sin su consentimiento para fines distintos de los indicados.

Introduce el Reglamento una especialidad para el caso de que se traten datos de menores de edad, lo cual es posible en una relación laboral siempre que el empleado tenga más de 16 años y pueda, por tanto, trabajar por cuenta ajena, de conformidad con los artículos 6 y 7 del Estatuto de los Trabajadores. Sin consentimiento de los representantes legales, se prohíbe al empresario recabar del menor datos relativos a los demás miembros del grupo familiar, como los que se refieran a la actividad profesional, información económica o posición social de sus padres o tutores.

Información

Antes de recabar los datos del trabajador en el ámbito de una relación laboral, el empleador deberá informarle acerca de que se incorporarán a un fichero del que la empresa es responsable, de la finalidad del tratamiento, de las cesiones de datos previstas y de los derechos de acceso, rectificación, cancelación y oposición que el afectado tiene, indicándole el modo en que puede ejercitarlos.

En el caso de menores de edad, dicha información ha de efectuarse en un lenguaje fácilmente comprensible y con expresa indicación de las limitaciones relativas a la prohibición de pedirles que faciliten datos de los demás miembros del grupo familiar.

Es recomendable que la información a los trabajadores sobre el tratamiento de sus datos personales se lleve a cabo por medios que permitan a la empresa conservar prueba de que se ha efectuado de modo idóneo, puesto que la carga de la prueba del cumplimiento del deber de informar corresponde al empleador. A tal fin, conviene que dicha información se incorpore a un documento que sea firmado por el trabajador a modo de recibí y que puede serle entregado en el mismo momento de la firma del contrato de trabajo.

Derechos de acceso, rectificación, cancelación y oposición de los trabajadores

Como el resto de personas cuyos datos forman parte de los ficheros de la empresa, los trabajadores tienen derecho a ejercer ante aquella los derechos de acceso, rectificación, cancelación y oposición que la Ley les reconoce, debiendo ser respondidos en tiempo y forma por el empresario. En la práctica, el ejercicio de estos derechos en

el seno de una relación laboral no es una excepción, ya que los trabajadores son cada vez más conscientes de los derechos que ostentan frente a la empresa.

Tratamiento por tercero de los datos de los trabajadores para la prestación de un servicio al empresario

Tiene especial relevancia la frecuente situación en la que el empleador decide subcontratar con un tercero especializado (asesoría laboral, gestoría, etc,) las tareas de elaboración y llevanza de nóminas y seguros sociales y de asesoramiento laboral general. Inevitablemente, el asesor laboral o la gestoría han de acceder a los datos personales de los trabajadores para la prestación de los servicios, por lo que los datos ya no sólo serán tratados por el empresario en el marco de la relación laboral, sino también por un tercero en nombre y por cuenta de aquel.

Estas situaciones son lícitas siempre y cuando, de conformidad con el artículo 12 de la LOPD, se suscriba entre el empresario y el asesor laboral un contrato en el que este, en su condición de encargado del tratamiento de los datos personales de los trabajadores por cuenta del empleador, asuma por escrito las siguientes obligaciones: tratar los datos únicamente para la finalidad para la que se le han entregado y conforme a las instrucciones del empleador, no comunicarlos a tercero sin autorización de este, cumplir las medidas de seguridad reglamentariamente exigidas y destruir o devolver al empresario los datos una vez finalizada la prestación de servicios.

Este acuerdo recibe técnicamente la denominación de Contrato de Acceso a Datos.

Como regla, el asesor laboral no podrá, a su vez, subcontratar con un tercero todo o parte de los servicios. No obstante, esta subcontratación sí será posible cuando concurra alguna de las dos circunstancias siguientes:

- Que el empleador le haya autorizado para efectuar la subcontratación en nombre y por cuenta de aquel.
- Que, no existiendo dicha autorización, se cumplan, acumulativamente, los siguientes requisitos:
  - Que en el Contrato de Acceso a Datos se especifiquen los servicios que se podrán subcontratar y la empresa subcontratista. Si esto último no fuera posible en el momento de celebrar el contrato, deberá comunicarse al empleador la identidad del subcontratista antes de la subcontratación.
  - Que el tratamiento de datos personales por el subcontratista se ajuste a las instrucciones del empresario.
  - Que el asesor laboral y el subcontratista firmen también un Contrato de Acceso a Datos en el que este asuma las obligaciones antes expresadas.

Finalizada la relación de prestación de servicios del asesor laboral a la empresa, aquel debe destruir o devolver a esta los datos personales de trabajadores que haya tratado en su nombre y por su cuenta. Si existiera una obligación legal de conservar los datos, deberán siempre devolverse al empleador, lo cual será aplicable a la documentación relativa al cumplimiento de deberes laborales del empresario, que deberá ser conservada durante los plazos establecidos en la normativa aplicable.

Teniendo en cuenta que de la prestación de servicios efectuada pueden derivarse responsabilidades, el asesor laboral podrá conservar los datos hasta que dichas responsabilidades prescriban. En tal caso, los datos personales habrán de conservarse bloqueados, es decir, identificados y reservados a disposición de las autoridades administrativas o judiciales competentes.

Medidas de seguridad

Si algo tiene de novedoso el Reglamento de desarrollo de la LOPD es lo relativo a la regulación de las medidas de seguridad que deben adoptarse en el tratamiento de los datos de carácter personal, regulando específicamente un aspecto que había sido olvidado en la antigua normativa: las medidas de seguridad que deben aplicarse al tratamiento de datos personales en soporte papel.

Ello tiene una aplicación inmediata en el ámbito del tratamiento de los datos personales de trabajadores, que, frecuentemente, se efectúa en soporte papel

(nóminas, *curricula vitae,* partes de baja, informes de prevención de riesgos laborales, etc.)

Aplicación de niveles de seguridad

El nuevo Reglamento, como lo hacía el antiguo, prevé tres niveles de seguridad distintos (básico, medio y alto) a aplicar en el tratamiento de datos personales. La exigibilidad de uno u otro nivel de seguridad dependerá del tipo de dato de que se trate en cada caso (nivel alto para datos más sensibles, básico para los menos).

Sigue vigente la regla de que es necesario aplicar un nivel alto de seguridad cuando se traten datos de minusvalías, salud o afiliación sindical, entre otros. Sin embargo, la nueva norma permite aplicar un nivel de seguridad básico cuando se dé alguna de las siguientes circunstancias:

- Que los datos se utilicen con la exclusiva finalidad de efectuar una transferencia dineraria a las entidades de las que el afectado sea miembro (lo cual es aplicable al tratamiento de datos de afiliación sindical del empleado con la finalidad de practicar la retención en nómina para abonar la cuota sindical).
- Que se trate de ficheros o tratamientos en papel en los que, de forma incidental o accesoria, se contengan aquellos datos, sin guardar relación con su finalidad.
- Que los datos que se traten se refieran al grado de discapacidad o condición de discapacidad o invalidez del afectado con motivo del cumplimiento de deberes públicos (como es el caso del tratamiento de estos datos para practicar la retención del IRPF en la nómina).

Una interpretación literal del Reglamento debe llevarnos a la conclusión de que seguirán estando sometidos a un nivel alto de seguridad los datos de salud de trabajadores (bajas por enfermedad, partes de confirmación de baja, documentos de las que dichas bajas sean deducibles, etc.).

Además, con la nueva norma, la tenencia por las empresas de *curricula vitae* con la finalidad de llevar a cabo procesos de selección de personal hará necesario, en muchos casos, aplicar a estos un nivel medio de seguridad, puesto que se impone para aquellos ficheros que contengan un conjunto de datos de los que puedan deducirse aspectos de la personalidad o el comportamiento, categoría a la que, sin duda, pertenecen muchos Curricula.

Por último, deberá aplicarse un nivel medio de seguridad en el tratamiento de datos relativos a infracciones o procedimientos disciplinarios seguidos contra los trabajadores, frecuentemente mantenidos por las empresas y sus gestorías.

Por lo limitado del espacio, el estudio de las concretas medidas aplicables a cada uno de los niveles de seguridad no puede ser desarrollado aquí. Baste con indicar que todas las empresas que traten datos de carácter personal deben tener un protocolo interno de seguridad, denominado documento de seguridad, en el que se describirán por escrito las medidas y procedimientos de seguridad a adoptar por la entidad.

El documento de seguridad debe describir tanto las medidas de seguridad a adoptar en el tratamiento de datos personales mediante sistemas informáticos, como las relativas a los documentos en papel que contengan datos de carácter personal.

El documento de seguridad es de cumplimiento obligatorio para la empresa y para sus trabajadores, debiendo adoptarse las medidas necesarias para que estos conozcan y comprendan las obligaciones que les afectan y las consecuencias en que pueden incurrir en caso de incumplimiento, lo que en la práctica se traduce en la posibilidad de exigir al empleado incumplidor las oportunas responsabilidades legales (disciplinarias, civiles e incluso, en ocasiones, penales).

Conclusiones

El Reglamento ha venido a aclarar algunas de las dificultades que, desde el punto de vista de la interpretación y aplicación práctica de la Ley, planteaba la normativa derogada, aunque también ha generado nuevos problemas, al adolecer de imprecisiones no deseables en una norma de rango reglamentario.

Su implantación va a suponer para las empresas un importante esfuerzo, en especial en lo que se refiere a las medidas de seguridad a aplicar con respecto a los datos personales que se traten en soporte papel. Es este uno de los ámbitos que más dificultades prácticas implicará, exigiendo inversiones y cambios organizativos que resultarán al principio tan engorrosos como, una vez implantados, beneficiosos para la empresa en términos de seguridad y eficacia.

El cumplimiento de la normativa de protección de datos personales es hoy para las empresas una obligación no sólo con consecuencias formales; de ella se obtienen indudables ventajas prácticas. El mercado demanda que los prestadores de servicios ofrezcan garantías de cumplimiento de la legalidad. Las empresas sólo ponen su información en manos de terceros que les ofrezcan seguridad y confidencialidad. Además, las cuantiosas multas que pueden imponerse en caso de infracción de esta normativa (hasta 600.000 €) hacen imprescindible su implantación integral si una empresa no quiere verse abocada, antes o después, a sufrir una sanción que, en el caso de las PYMES, no pocas veces obliga al cierre del negocio.

Ciertamente, la implantación y aplicación práctica de la LOPD en las empresas no es sencilla. Por ello, se hace muy recomendable contar con la asistencia de especialistas en la materia que no sólo auxilien al empresario en el proceso de implantación, sino que faciliten la puesta en práctica de las medidas legales y que adapten estas a las características y necesidades propias de cada empresa. En este campo, como en otros, la externalización de servicios no sólo es recomendable, por razones de economía y eficacia, sino, en la mayoría de ocasiones, imprescindible. El desembolso inicial que ello supone para la empresa se traduce inmediatamente en importantes beneficios, tanto internos: incremento de la seguridad, garantía de confidencialidad, aumento de la eficacia y mejora de los procesos de gestión de la información; como externos: mejora de la imagen de empresa en el mercado, obtención de ventajas competitivas y evitación del riesgo de sufrir denuncias y sanciones.

[La jurisprudencia responde]

La calificación del despido por enfermedad del trabajador: una cuestión zanjada, al menos judicialmente

Ricardo Morón Prieto

Prof. Titular de Derecho del Trabajo y de la Seguridad Social
Universidad Autónoma de Madrid

Introducción y antecedentes

El Tribunal Supremo ha dictado recientemente dos sentencias con las que parece haber zanjado, por el momento y en el ámbito judicial, la cuestión referida a la calificación de los despidos basados en la morbilidad del trabajador. La cuestión debatida se circunscribe no a la licitud o ilicitud del despido por enfermedad del trabajador –que, en la medida en que no se atenga a las previsiones del art. 52.d) del Estatuto de los Trabajadores (ET), ha de ser declarado ilícito- sino a la calificación de la actuación empresarial como improcedente o nula. La opción está notablemente condicionada por dos aspectos: uno de índole legal, que es la precisión -limitación- con la que nuestro ordenamiento configura la posibilidad de declaración de nulidad del despido, limitado desde las reformas de 1990 y 1994 exclusivamente a los supuestos en que este tenga por móvil alguna de las causas de discriminación prohibidas en la Constitución o en la Ley, o bien se produzca con violación de derechos fundamentales o libertades públicas del trabajador (art. 55.5 ET). Ello implica que cualquier despido ilícito que no tenga tales móviles solo podrá ser declarado improcedente. El otro