Informe 0574/2009

La consulta plantea diversas dudas respecto a la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), a la prestación de un servicio de alojamiento, en un servidor de la empresa consultante, de bases de datos de empresas clientes que contienen datos de carácter personal.

I

Con carácter general, cabe señalar que la empresa consultante como prestadora del servicio de hosting se configura como encargado de tratamiento, en el sentido del apartado 3.g) de la LOPD, que lo define como "*La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".*

Ello sucederá siempre que la empresa que presta el servicio de alojamiento no pueda en modo alguno decidir sobre el contenido, finalidad y uso del tratamiento y siempre que su actividad no le reporte otro beneficio que el derivado de albergar las bases de datos, sin utilizarlas en modo alguno en su provecho, puesto que en ese caso pasaría a ser responsable del fichero, existiendo una cesión de datos de carácter personal que, tal y como exige el artículo 11.1 de la LOPD, requerirá el consentimiento de los afectados.

La LOPD regula la figura del encargado del tratamiento en su artículo 12 al establecer: "*No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento".*

A este respecto, el Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa en el último apartado del número primero del artículo 20 que "*No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado*. "

Para que la relación entre responsable y encargado del tratamiento pueda darse y se ajuste a la Ley, es preciso que se cumplan los requisitos expresados en el artículo 12 de la LOPD, considerando los siguientes aspectos:

En primer lugar, es preciso que el acceso a los datos por el tercero se efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero, y que dicha relación de servicios se encuentre contractualmente establecida. En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 de la LOPD impone que "*la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".*

El hecho de que la relación derivada del contrato sea la existente entre un responsable y un encargado del tratamiento implicará que al término de la relación sea aplicable lo establecido en el artículo 12.3 de la LOPD, de forma que "*una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".*

El incumplimiento de esta previsión llevará aparejada la consecuencia, prevista en el artículo 12.4 de la LOPD, de que *"En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".*

Esta Agencia Española de Protección de Datos ha venido indicando que el deber de devolución al que se refiere el artículo 12.3 de la LOPD podrá verificarse mediante la entrega directa de los datos al propio responsable del tratamiento o mediante la realización de dicha entrega al encargado del tratamiento que este designase, toda vez que en este segundo caso el encargado actuaría como mero mandatario del responsable, siendo precisamente éste el que establece a quién han de entregarse los datos en su nombre y por su cuenta. Y así se recoge en el artículo 20.3 del Reglamento antes citado "*no obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique*

los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo."

Por su parte, el artículo 22 del aludido Reglamento dispone respecto de la conservación de los datos lo siguiente:

"*1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.*

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento."

II

En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículo 9 y 12.2 de la LOPD.

El Reglamento de desarrollo de la Ley Orgánica 15/1999, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, el nivel correspondiente en función de la naturaleza de los datos a tratar. Debe tenerse presente, además, que dichas medidas tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.

De esta manera el encargado de tratamiento deberá aplicar a cada fichero o sistema de información de cada una de las entidades clientes las medidas de seguridad correspondientes según el tipo de datos a tratar. En el presente caso, cabe destacar que en la consulta se indica que en la aplicación de gestión de centros de la tercera edad, se van a tratar muy diversos datos,

entre los que se encuentran datos relativos a la medicación, tratamientos y grado de dependencia del residente, todos ellos datos de salud de conformidad con lo dispuesto en el artículo 5.1.g) del Reglamento que define a éstos como "*las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética*." Los ficheros que contengan este tipo de datos estarán sujeto a medidas de seguridad de nivel alto, tal y como establece el artículo 81.3 del Reglamento, según el cual "*Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual."*

No obstante debe recordarse aquí que el artículo 81.8 del citado Reglamento permite aplicar diferentes niveles de seguridad a un fichero o un sistema de información siempre que se den las condiciones que dicho precepto exige. Dispone dicho artículo: "*A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad."*

Entre las obligaciones del encargado del tratamiento en materia de medidas de seguridad se encuentra la de elaborar el correspondiente documento de seguridad, tal y como establece el articulo 82.2 del Reglamento según el cual *"Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento."*

En cuanto al modo de acceso a los datos, se señala en la consulta que cada usuario accede a la aplicación a través de un "usuario y contraseña", debiendo recordarse aquí que el artículo 85 del Reglamento prevé respecto del acceso a datos a través de redes de comunicaciones que "*Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80."*

En este sentido, el artículo 91 del Reglamento impone ya desde el nivel básico una obligación de control de acceso, disponiendo en su número primero que "*Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones",* para ello exige en su número tercero que *"El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados."*

Asimismo, establece una obligación de identificación y autenticación de los usuarios, exigiéndose igualmente desde el nivel básico una identificación personalizada de los usuarios. Dispone el artículo 93.1, a estos efectos, que "*El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios*." Por su parte, el número 2 del mismo artículo prevé que "*El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado."*

En el nivel medio, esta medida de identificación y autenticación se vuelve más rigurosa ya que, a las medidas anteriores previstas para el nivel básico, se añade la contenida en el artículo 98 según el cual "*El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información."*

En el nivel alto, se requiere ya un registro de cada intento de acceso que se produzca, establece el artículo 103.1 que "*De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado*." Mientras que el número segundo del mismo artículo dispone "*En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido."*

Por consiguiente, respecto de los ficheros sujetos a medidas de seguridad de nivel alto, dado su carácter acumulativo, además de la identificación inequívoca y personalizada del usuario autorizado y la limitación del intento de accesos a que se refiere el artículo 98, se requiere la existencia de un registro de accesos en los términos establecidos en el artículo 103, cuya función es determinar quien ha intentado acceder a un determinado fichero en cada momento, si ha sido autorizado para ello, y en su caso, cual es el registro accedido.

Por último, debe tenerse en cuenta en el presente supuesto lo previsto en el artículo 104 del Reglamento respecto de la trasmisión de datos a través de redes de comunicaciones, según el cual "*Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de*

datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros."

III

Se consulta, asimismo, si es precisa una autorización del residente en un centro de tercera edad para que sus familiares puedan conocer a través de una página web su situación desde el punto de vista de los servicios que se le han prestado o su estado de salud.

A este respecto cabe señalar que la comunicación de dichos datos a los familiares constituye una cesión de datos de carácter personal, definida en el artículo 3 i) de la LOPD como "*Toda revelación de datos realizada a una persona distinta del interesado".*

Tal cesión debe sujetarse al régimen general de comunicación de datos de carácter personal establecido en el artículo 11 de la misma Ley, conforme al cual *"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."*

En lo que se refiere a los datos de salud, debe además recordarse que el tratamiento y cesión de datos de carácter personal, cuyo régimen aparece recogido con carácter general en los artículos 6 y 11 de la LOPD, se encuentra, por vía de excepción, sometido a particulares restricciones en lo que a los datos de salud respecta, por el artículo 7 de la citada Ley Orgánica, cuyo apartado 3 establece como regla general que "*Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente"*. Esta regla únicamente es matizada por la LOPD en sus artículos 7.6 y 8

Por consiguiente en el presente supuesto, será preciso el consentimiento del residente, consentimiento que deber reunir las características enumeradas en el artículo 3.h de la LOPD, que lo define como una "*manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*", a ello debe añadirse que, en el caso de datos relativos a la salud, debe ser expreso, tal y como indica el artículo 7 de la LOPD.

El deber de información viene regulado en el artículo 5.1 de la LOPD según el cual ***"****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."*

Conforme a lo establecido en el último inciso del artículo 12.2 del Reglamento la prueba de que se ha producido el consentimiento, que corresponderá al responsable del fichero o tratamiento, en el caso sometido a consulta el centro de la tercera edad, podrá hacerse por cualquier medio de prueba admisible en derecho. Debe tenerse en cuenta que, en el caso de los datos de salud, si bien el consentimiento debe ser expreso, el número tercero del artículo 7 de la LOPD no exige que se produzca por escrito, a diferencia de lo previsto en el apartado segundo del mismo artículo para los datos relativos a ideología, afiliación sindical, religión y creencias. No obstante, resulta indudablemente más sencillo para el responsable del fichero o tratamiento la acreditación del consentimiento cuando éste se realiza por dicho procedimiento.

Asimismo, debe tenerse en cuenta que el artículo 18 del Reglamento de desarrollo de la LOPD impone al responsable del fichero o tratamiento la obligación de acreditar el cumplimiento del deber de información disponiendo lo siguiente "*1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.*

2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales."