



La consulta plantea numerosas dudas en relación con la aplicación de lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, a la constitución de un portal web privado y de acceso restringido como medio complementario de rendición de cuentas por la administración de la comunidad.

Con carácter previo debe indicarse que el presente informe se referirá exclusivamente al tratamiento y cesión de datos personales contenidos en documentos de la comunidad de propietarios, sin que esta a Agencia competa resolver cuestiones en relación con la documentación que no contenga datos personales.

I

Debe así, en primer término, delimitarse el concepto de dato personal. A este respecto debe indicarse que los artículos 1 y 2 de la Ley Orgánica 15/1999, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como *“cualquier información concerniente a personas físicas identificadas o identificables.”*

El Grupo Trabajo del artículo 29, órgano consultivo independiente de la Unión Europea 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 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, señalaba en su dictamen en su Dictamen 4/2007, sobre el concepto de datos personales, que, desde el punto de vista del contenido de la información, el concepto de datos personales incluye todos aquellos datos que proporcionan información cualquiera que sea la clase de ésta. Por supuesto esto incluye la información personal considerada «datos sensibles» en el artículo 8 de la Directiva a causa de su naturaleza particularmente delicada, pero también otras categorías más generales de información. El término «datos personales» comprende la información relativa a la vida privada y familiar del individuo stricto sensu, pero también la información sobre cualquier tipo de actividad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social. El concepto de «datos personales» abarca, por lo tanto, información sobre las personas, con independencia de su posición o capacidad (como consumidor, paciente, trabajador por cuenta ajena, cliente, etc.).



El Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa que constituye un dato de carácter personal *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.”*

Por consiguiente, en la documentación a que la consulta se refiere se encontrarán numerosas informaciones que constituyen datos personales, tales como datos identificativos y de contacto de los propietarios, números de sus cuentas corrientes, coeficientes de participación, consumos individuales, ingresos efectuados por los propietarios o deudas que estos mantengan con la comunidad, sentido del voto en la adopción de acuerdos, etc. Igualmente cualquier dato referido a los empleados que pudiera tener la comunidad de propietarios, tendrán dicha consideración, como también la tendrán los datos relativos a honorarios de profesionales que abone la comunidad.

II

La comunicación a los diferentes propietarios, por parte de los Órganos de Gobierno de la comunidad de propietarios, de datos personales contenidos en la documentación que obra en poder de la misma, implicará una cesión de datos de carácter personal, definida por el artículo 3.i) de la Ley Orgánica 15/1999, como *“toda revelación de datos realizada a una persona distinta del interesado”*.

En relación con esta cuestión, el artículo 11.1 de la citada Ley 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”*, estableciendo en el artículo 11.2 una serie de excepciones, de las cuales interesa a efectos del presente supuesto la contenida en el apartado a) que prevé la posibilidad de cesión no consentida *“cuando la cesión esté autorizada por una Ley”*.

Por ello, será posible admitir la cesión de los datos sin consentimiento del interesado en aquellos supuestos en los que exista una norma con rango de Ley, que habilite esta cesión.

A este respecto, la propia Ley 49/1960, de 21 de julio, de Propiedad Horizontal, habilita diversas cesiones de datos personales, así el artículo 16.2) regula como debe efectuarse la convocatoria de las juntas, disponiendo que *“La convocatoria contendrá una relación de los propietarios que no estén al corriente en el pago de las deudas vencidas a la comunidad y advertirá de la privación del derecho de voto si se dan los supuestos previstos en el artículo 15.2.”*

Igualmente, el artículo 19 prevé la remisión de las actas a los propietarios, señalando en su número segundo las menciones que debe contener, entre las que figuran varios datos personales, dispone dicho precepto que *“2. El acta de cada*

reunión de la Junta de propietarios deberá expresar, al menos, las siguientes circunstancias:

- *a) La fecha y el lugar de celebración.*
- *b) El autor de la convocatoria y, en su caso, los propietarios que la hubiesen promovido.*
- *c) Su carácter ordinario o extraordinario y la indicación sobre su celebración en primera o segunda convocatoria.*
- *d) Relación de todos los asistentes y sus respectivos cargos, así como de los propietarios representados, con indicación, en todo caso, de sus cuotas de participación.*
- *e) El orden del día de la reunión.*
- *f) Los acuerdos adoptados, con indicación, en caso de que ello fuera relevante para la validez del acuerdo, de los nombres de los propietarios que hubieren votado a favor y en contra de los mismos, así como de las cuotas de participación que respectivamente representen.”*

Asimismo, el artículo 20 señala entre las funciones del secretario la de “custodiar a disposición de los titulares la documentación de la comunidad.” En cuanto a cómo debe interpretarse este precepto desde la óptica de la protección de los datos personales, cabe recordar que reiteradamente esta Agencia ha señalado en sus informes que el hecho de que una norma con rango de Ley habilite el tratamiento o cesión de los datos no resulta por sí solo suficiente para considerar dicho tratamiento o cesión, sin más, como amparados por la Ley Orgánica 15/1999, siendo igualmente preciso que los mismos resulten conformes a lo dispuesto en la mencionada Ley y en particular a los principios de proporcionalidad y finalidad consagrados por su artículo 4.1.

Dispone el citado artículo 4.1 de la Ley Orgánica 15/1999 que “Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.”

Por consiguiente, la comunicación de datos deberá limitarse a aquellos datos que en cada caso resultan “adecuados, pertinentes y no excesivos” para el cumplimiento de la finalidad que legitima el acceso a los mismos, que en el presente supuesto viene referido al control del buen gobierno de la comunidad de propietarios.

Respecto de la proporcionalidad ha señalado el Tribunal Constitucional en la Sentencia 207/1996 que se trata de “una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales(...) En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de

conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)”.

Así, cabe señalar, a título de ejemplo, que no cumple el requisito de idoneidad la comunicación de los directorios con los datos de domicilio de los propietarios o sus números de cuenta corriente, en tanto que en nada contribuyen a la finalidad de control de la buena administración de la comunidad de propietarios. Igualmente, y en lo que se refiere a nóminas de los empleados de la comunidad, debe tenerse en cuenta que junto con la información referida a sus retribuciones, aparecerán otros datos, como el domicilio fiscal de los interesados, la cuenta corriente en que se produzca los pagos e incluso datos especialmente protegidos si se refieren a salud o ideología, como el descuento, en su caso, de la cuota sindical de los afiliados a un sindicato, etc. Estos datos no resultan relevantes para la finalidad de control de la gestión de la comunidad, por lo que la exhibición de los directorios antes citados o las nóminas de personal resultará contraria al principio de proporcionalidad y, en consecuencia, darán lugar a una vulneración de lo previsto en la Ley Orgánica 15/1999, sin perjuicio de que se deba informar a los propietarios de las retribuciones satisfechas a los empleados, con el adecuado desglose de conceptos retributivos.

De este modo el artículo 20 de la Ley de propiedad Horizontal, debe ser interpretado de conformidad con las previsiones de la Ley Orgánica 15/1999, de modo que no permite un acceso generalizado a toda la documentación obrante en los archivos de la comunidad que puedan contener datos personales, sino solamente a aquellos datos que sean estrictamente pertinentes y adecuados para la finalidad perseguida, por lo que fuera de los supuestos en los que expresamente la Ley de propiedad horizontal obliga a la comunicación a otros propietarios de determinados datos personales, deberá en cada caso valorarse si la comunicación de datos de carácter personal resulta conforme al principio de proporcionalidad, examinando si resulta idónea, necesaria y equilibrada tal y como señala la mencionada sentencia del Tribunal Constitucional, no procediendo la comunicación de aquellos documentos en que se revelen datos personales de manera contraria al principio de proporcionalidad.

Por otra parte, la finalidad del tratamiento no podrá ser otra que la que resulte de las previsiones de la Ley de Propiedad horizontal, esto es, comunicación de que se va a celebrar una junta de propietarios dando, en su caso, conocimiento de aquéllos a los que se limita el derecho a voto, conocimiento de los acuerdos adoptados y las mayorías con que lo fueron y, en el caso en que fuera relevante, el sentido del voto. En cuanto a la comunicación de otros datos personales obrantes en los ficheros de la comunidad en virtud de lo establecido en el artículo 20 de la Ley, su finalidad será, con carácter general, la de control de la gestión que se lleva a



cabo de la comunidad. Dispone el así el artículo 4.2 de la Ley Orgánica 15/1999 que los datos *“no podrán utilizarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”*. Debe aclararse aquí que la Audiencia Nacional partiendo de una interpretación sistemática de este precepto viene considerando la expresión “finalidades incompatibles” como sinónimo de “finalidades distintas”. De esta manera, cualquier utilización de los datos personales con fines distintos de los autorizados en dicha Ley supondría una vulneración de la citada Ley Orgánica.

Debe tenerse en cuenta, asimismo, que el artículo 10 de la Ley Orgánica 15/1999 sujeta al responsable del fichero, esto es a la propia comunidad de propietarios, a un deber de secreto, deber al que se encuentran igualmente sometidos los propietarios como miembros de la Junta de propietarios. Dispone dicho artículo 10 que *“El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.”* El incumplimiento de este deber es constitutivo de infracción de la Ley Orgánica 15/1999.

III

Todo tratamiento de datos de carácter personal deberá ser respetuoso de los principios contenidos en la Ley Orgánica 15/1999, pero en el supuesto de que se cree por la comunidad de propietarios un portal web, con la finalidad de poner a disposición de todos los propietarios documentos cuya custodia está encomendada al administrador, debe tomarse en consideración que la utilización de las nuevas tecnologías tiene una gran incidencia en el derecho a la protección de datos personales, por lo que debe darse un especial énfasis al cumplimiento de los restantes principios recogidos en el artículo 4 de la Ley Orgánica 15/1999.

De este modo cabe recordar que el artículo 4.3 dispone respecto del principio de exactitud que *“Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.”* Por su parte, el artículo 4.5 se refiere al principio de conservación disponiendo 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.”

De este modo los datos personales que figuren en el portal deberán estar siempre actualizados y permanecer en el mismo solamente durante el tiempo necesario para el cumplimiento de la finalidad que en cada caso resulte de lo



previsto en la Ley de Propiedad Horizontal, debiendo eliminarse cuando la finalidad se encuentre cumplida, sin perjuicio de que el administrador, al que la Ley atribuye una función de custodia de la documentación, mantenga la misma en otros soportes durante los plazos que legalmente proceda.

IV

El artículo 9 de la Ley Orgánica 15/1999 exige que el responsable del fichero, y, en su caso, el encargado del tratamiento adopten *“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.”* Dicho artículo prohíbe en su número segundo el registro de 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 en la actualidad reguladas en el Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, 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.

Deberán así adoptarse respecto al portal todas las medidas de seguridad aplicables a ficheros y tratamientos automatizados, según la naturaleza de los datos tratados.

De ellas debe destacarse la recogida con carácter general en el artículo 85, según la cual *“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.”*

Cabe igualmente recordar la necesidad de modificar el documento de seguridad, como consecuencia de la creación del portal. Señala a este respecto el artículo 88.7 que *“El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.”*



En la adopción de las medidas de carácter básico debe resaltarse la establecida en el artículo 89, según el cual, el responsable del fichero, esto es la comunidad de propietarios, deberá adoptar las medidas necesarias para que las personas que accedan a los datos, en el presente caso los diferentes propietarios, conozcan las normas de seguridad y las consecuencias que conlleva su incumplimiento. De la misma manera, debe tenerse especialmente en cuenta la necesidad de llevar un registro de incidencias, en la forma prevista en el artículo 90, y las medidas relativas al control de accesos y a la identificación y autenticación de los usuarios. Dispone respecto de ésta últimas el artículo 93 que *“1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.*

2. 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.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible. “

V

La Ley Orgánica 15/1999 atribuye al afectado por un tratamiento de datos el derecho a utilizar un conjunto de mecanismos reactivos que constituyen una parte del contenido esencial del derecho fundamental a la protección de datos. Estos mecanismos se concretan en los derechos de acceso, rectificación, cancelación y oposición regulados en los artículos 15 y siguientes de la Ley.

En lo que se refiere a los derechos de rectificación y cancelación prevé el artículo 16.2 de la Ley Orgánica que *“Serán rectificadas o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.”*

Debe señalarse que ambos derechos se encuentran vinculados al incumplimiento por parte del responsable del fichero, en este caso, el titular del portal, de los principios consagrados en el artículo 4 de la Ley Orgánica 15/1999, en particular los de actualización, exactitud y conservación, aunque la rectificación o cancelación puede proceder de la conculcación de cualquiera de los principios enumerados en dicho artículo, de este modo procederá otorgar el citado derecho cuando se esté produciendo el tratamiento de datos excesivos en relación con la finalidad que justifica aquél tratamiento, así como cuando los datos se estén empleando para fines incompatibles con el que justificó su recogida y tratamiento o

cuando los datos hayan sido conservados y no cancelados por un período superior al derivado de la finalidad por la que se trataron o, evidentemente, cuando los datos no resulten exactos ni respondan, tal y como exige el artículo 4.3 de la Ley Orgánica 15/1999 a la situación actual del afectado.

En el presente supuesto, en que los datos se tratan sin consentimiento del interesado, resulta especialmente relevante lo previsto respecto al derecho de oposición. El artículo 6.4 establece al respecto que *“En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable de fichero excluirá del tratamiento los datos relativos al afectado.”*

Por consiguiente, el afectado por el tratamiento de datos podrá ejercitar los derechos que la Ley Orgánica 15/1999 le concede, que no podrán denegarse cuando se produzca alguna de las circunstancias en que dicha Ley determina la posibilidad de su ejercicio. Debe así recordarse que un tratamiento de datos hasta ese momento lícito puede devenir ilícito si no se atiende a las especiales circunstancias invocadas por el interesado al tiempo de ejercitar su derecho.

Añade el artículo 18.2 de la Ley Orgánica 15/1999 que *“el interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o, en su caso, del organismo competente de cada Comunidad autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación”*.

De esta manera, las personas físicas cuyos datos se encuentren en el portal a que hace referencia la consulta podrán ejercitar sus derechos de acceso, rectificación, cancelación u oposición ante la comunidad de propietarios titular del portal, derechos que deberán ser atendido en los plazos fijados en la ley Orgánica 15/1999 y en su Reglamento de desarrollo, en otro caso, podrán recabar la tutela de esta Agencia en la forma prevista en el artículo 18 de la citada ley Orgánica. Debe señalarse que el ejercicio de estos derechos no se encuentra restringido a los usuarios del portal sino que corresponde a cualquier persona cuyos datos se traten en el mismo.

VI

La creación de un portal por un grupo reducido de propietarios en el que se tratarán datos personales contenidos en la documentación obrante en los ficheros de la comunidad de propietarios a la que pertenecen, convertirá a los propietarios que formen parte de dicho grupo en responsables de un fichero, a los que, en consecuencia, resultará exigible el cumplimiento de las obligaciones impuestas a

estos por la Ley Orgánica 15/1999 y responderán de los incumplimientos de dicha norma, sin que sus actuaciones puedan ser imputadas a la comunidad.

Para que pudiera realizarse el tratamiento pretendido, sería preciso que se encontrasen legitimados para ello, dado que, para que el tratamiento de los datos de carácter personal sea lícito, el artículo 6.1 de la Ley Orgánica 15/1999 establece que *“el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”*. Debe señalarse aquí que la legitimación en el presente caso no puede enmarcarse en las facultades y obligaciones que a la comunidad de propietarios atribuye la Ley de Propiedad Horizontal, de modo que no podrán incorporarse datos personales en dicho portal sin el consentimiento de cada uno de los afectados por el tratamiento de los datos.

A este respecto, no cabe considerar que nos encontremos ante una custodia conjunta de la documentación de la comunidad como señala el consultante, toda vez que esa función se atribuye en el artículo 20.e) de la Ley de Propiedad Horizontal al administrador. En este sentido, el artículo 13 de dicha Ley prohíbe que con la creación de otros órganos de gobierno en los Estatutos o por acuerdo mayoritario de la junta de propietarios, se menoscaben las funciones y responsabilidades frente a terceros que la propia Ley atribuye a los órganos de gobierno en ella establecidos y regulados.

En lo que se refiere al encargado del tratamiento, el artículo 5.1.i del Reglamento de desarrollo de la Ley Orgánica 15/1999 le define como *“La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.”*

En este sentido debe señalarse que para que la relación entre responsable y encargado del tratamiento se ajuste a la Ley Orgánica 15/1999, es preciso que se cumplan los requisitos exigidos en el artículo 12 de dicha norma, 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, esto es a la comunidad de propietarios 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 Ley Orgánica 15/1999 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 dicha Ley Orgánica, 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 misma norma, 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”.*

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 artículos 9 y 12.2 de la Ley Orgánica 15/1999.

Por consiguiente, solamente en el caso de que la comunidad de propietarios decida encomendar a un tercero, con independencia de que este pueda ser miembro de la propia comunidad de propietarios, la creación del portal objeto de consulta dando cumplimiento a los requisitos establecidos en artículo 12 de la Ley Orgánica 15/1999 podrá considerarse que existe dicha relación de encargo del tratamiento.

VII

Por último, teniendo en cuenta que en la consulta se hace referencia al almacenamiento de datos en la nube, debe hacerse una referencia a los problemas que plantea el servicio de cloud computing en materia de protección de datos personales.

Como punto de partida debe tomarse en cuenta lo señalado por el Grupo de trabajo del artículo 29 en su Dictamen 5/2012 sobre la computación en nube, en que analiza los riesgos específicos que puede generar el tratamiento de datos personales en la nube, dividiendo éstos en dos categorías: la falta de control sobre los datos y la falta de transparencia, esto es, la insuficiente información sobre la propia operación de tratamiento.

En lo que a la falta de control se refiere, señala el Dictamen aludido que “Al introducir datos personales en los sistemas gestionados por un proveedor, los clientes de servicios de computación en nube (en lo sucesivo, «clientes») pueden no

seguir teniendo el control exclusivo de estos datos y no pueden aplicar las medidas técnicas y de organización necesarias para garantizar la disponibilidad, integridad, confidencialidad, transparencia, aislamiento, posibilidad de intervención y portabilidad de los datos. Esta falta de control puede manifestarse de la siguiente manera:

- Falta de disponibilidad debido a la falta de interoperatividad (dependencia respecto del proveedor): si el proveedor se basa en tecnología patentada, puede resultar difícil para un cliente mover los datos y documentos entre diferentes sistemas en la nube (portabilidad de los datos) o intercambiar información con entidades que utilicen servicios de computación en nube gestionados por distintos proveedores (interoperatividad).
- Falta de integridad causada por la puesta en común de los recursos: una nube se compone de sistemas e infraestructuras comunes. Los proveedores tratan datos personales procedentes de una amplia gama de interesados y organizaciones, y es posible que surjan conflictos de intereses u objetivos diferentes.
- Falta de confidencialidad por lo que respecta a las solicitudes de intervención legal realizadas directamente a un proveedor: los datos personales tratados en la nube pueden ser objeto de solicitudes de intervención legal por parte de las autoridades policiales o judiciales de los Estados miembros de la UE y de terceros países. Existe el riesgo de revelación de datos personales a servicios incluso extranjeros sin una base jurídica de la UE válida y, por tanto, se daría una violación de la legislación de la UE sobre protección de datos.
- Falta de posibilidad de intervención debido a la complejidad y la dinámica de la cadena de subcontratación: el servicio de computación en nube ofrecido por un proveedor puede realizarse combinando servicios de varios proveedores distintos, que pueden añadirse o suprimirse dinámicamente a lo largo de la duración del contrato del cliente.
- Falta de posibilidad de intervención (derechos de los interesados): un proveedor no podrá aportar las medidas e instrumentos necesarios para ayudar al responsable del tratamiento a gestionar los datos en términos de, por ejemplo, acceso, supresión o corrección.
- Falta de aislamiento: un proveedor podrá ejercer su control físico sobre los datos de distintos clientes para vincular los datos personales. Si se proporciona a los administradores derechos de acceso suficientemente privilegiados (funciones de alto riesgo), podrían vincular información de distintos clientes. “



En lo que atañe a la falta de información sobre el tratamiento (transparencia) el Dictamen afirma que “La falta de información sobre las operaciones de tratamiento de un servicio de computación en nube plantea un riesgo para los responsables del tratamiento y para los interesados, que pueden no ser conscientes de las amenazas y riesgos potenciales y por tanto no podrán adoptar las medidas que consideren apropiadas. Algunas posibles amenazas pueden derivarse de que el responsable del tratamiento no sepa que:

- Se realiza un tratamiento en cadena con múltiples encargados del tratamiento y subcontratistas.
- Los datos personales se tratan en diferentes zonas geográficas del EEE. Ello incide directamente en la legislación de protección de datos aplicable a los litigios que puedan surgir entre usuario y proveedor.
- Se transmiten datos personales a terceros países no pertenecientes al EEE. Los terceros países pueden no proporcionar un nivel adecuado de protección de datos y las transferencias pueden no contar con las medidas de protección adecuadas (por ejemplo, cláusulas contractuales estándar o normas empresariales vinculantes) y, por tanto, esto puede ser ilegal.”

Por consiguiente, deben tomarse en consideración dichos riesgos cuando se contrata un servicio de cloud computing, teniendo en cuenta que dicha contratación no altera la condición de responsable del tratamiento de quien contrata, de modo que dicha responsabilidad no se desplaza al proveedor del servicio aunque sea una gran compañía multinacional o incorpore una cláusula al respecto.

En cuanto a la normativa de protección de datos aplicable será la del país en que esté establecido el responsable del tratamiento que contrata los servicios de computación en nube y no la del lugar en que se encuentren los proveedores de dichos servicios.

Por su parte, los proveedores de dichos servicios tendrán la condición de encargados del tratamiento, por lo que la relación entre responsable del fichero, y la entidad prestadora de servicios de cloud computing, deberá formalizarse en un contrato en los términos establecidos por el artículo 12 de la Ley Orgánica 15/1999.

Ahora bien, como indica el grupo de trabajo en el Dictamen a que se viene haciendo referencia “En la actual situación de la computación en nube, los clientes de estos servicios pueden no tener margen de maniobra a la hora de negociar las condiciones de uso de los mismos, ya que las ofertas normalizadas son una característica de muchos servicios de computación en nube. No obstante, en última instancia, es el cliente quien decide sobre la asignación de parte o de la totalidad de las operaciones de tratamiento a los servicios en nube con fines específicos; la función del proveedor de estos servicios será la de contratista frente al cliente, que



es el punto clave en este caso. Tal como se recoge en el Dictamen 1/2010 del GT 29 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», *«el desequilibrio en cuanto al poder contractual entre un pequeño responsable del tratamiento y un gran proveedor de servicios no debería considerarse una justificación para que el primero acepte cláusulas y condiciones de contratos que no se ajusten a la legislación en materia de protección de datos»*. Por esta razón, el responsable del tratamiento debe elegir un proveedor que garantice el cumplimiento de la legislación sobre protección de datos”

De ahí que en dicho Dictamen se señale que las entidades que deseen utilizar la computación en nube deben efectuar, como primer paso, un análisis de riesgos completo y riguroso, teniendo en cuenta su condición de responsable del tratamiento. El Dictamen les recomienda que seleccionen un proveedor de servicios de cloud computing que garantice el cumplimiento de la legislación sobre protección de datos, y que verifiquen si el proveedor de tales servicios puede garantizar la legalidad de las transferencias internacionales de datos. Debe así tenerse en cuenta, que, como pone de relieve el Grupo de Trabajo internacional de Berlín sobre protección de datos en las telecomunicaciones, en el Memorándum Sopot adoptado en 2012, en el que se analizan cuestiones relativa a la intimidad y protección de datos en la computación en nube, ésta no debe conducir a una disminución de los niveles de protección de datos en comparación con el tratamiento convencional

Esta Agencia ha publicado una guía, que se encuentra disponible en su página web, para facilitar la contratación de servicios de cloud computing, en la que se analizan las diversas cuestiones que dichos servicios plantean desde el punto de vista de protección de datos y se formulan recomendaciones a los responsables del tratamiento.

No obstante, debe tenerse especialmente en cuenta que, el modelo de *cloud computing* hace posible que tanto los proveedores de servicios como los datos almacenados en la *nube* se encuentren ubicados en cualquier punto del planeta. De este modo, como consecuencia del encargo del tratamiento o de las sucesivas subcontrataciones que el proveedor de servicios realiza, puede originarse una transferencia internacional de datos, el artículo 5.1 s) del Reglamento de desarrollo de la Ley Orgánica 15/1999, define estas como el *“tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español”*.

La transmisión de datos a entidades situadas fuera del Espacio Económico Europeo constituirá una transferencia internacional de datos que deberá respetar el régimen establecido en los artículos 33 y 34 de la Ley Orgánica 15/1999 y en el Título VI de su Reglamento de desarrollo.

Dispone a este respecto el artículo 33.1 de la Ley Orgánica 15/1999 que *“no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas”*.

El artículo 33.2 de la LOP establece los criterios para determinar el carácter adecuado de protección al disponer que *“el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países”*. En este sentido cabe recordar que la Comisión de la Unión Europea ha adoptado decisiones en las que se ha considerado que existe un nivel adecuado de protección en Estados tales como Suiza, Argentina, Uruguay, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos y las entidades estadounidenses adheridas a los «principios de Puerto Seguro».

En consecuencia, el responsable que contrata un servicio de cloud computing, debe conocer la cadena de subcontrataciones a fin de estar informado donde pueden localizarse los datos y si el país tiene un régimen de garantías adecuado, debiendo solicitar la correspondiente autorización de la Agencia en caso contrario. Señala en este sentido el Dictamen 5/2012 que la transparencia en la nube supone que es necesario que el cliente tenga conocimiento de todos los subcontratistas que contribuyan a la prestación de los respectivos servicios en nube, así como de la localización de todos los centros donde puedan tratarse los datos personales. Sólo entonces podrá evaluar si los datos personales pueden ser transferidos a un llamado tercer país fuera del Espacio Económico Europeo (EEE) que no garantice un nivel adecuado de protección en el sentido de la Directiva 95/46/CE.

Por consiguiente, debe tenerse presente al contratar un servicio de cloud computing los aspectos relativos a las transferencias internacionales de datos y, en particular, en caso de que se produzcan transferencias de datos a EEUU debe comprobarse que los subcontratistas en dicho país están adheridos a los principios de Puerto Seguro para la prestación de dichos servicios de cloud computing.